世界数学名题欣赏丛书

希尔伯特第十问题

胡久稔 编著

辽宁教育出版社

1987年·沈阳

希尔伯特第十问题

胡久稔　编著

辽宁教育出版社出版　辽宁省新华书店发行
(沈阳市南京街6段1里2号)　沈阳新华印刷厂印刷

字数:100,000　开本:$787\times1092\ ^1/_{32}$　印张:$6\ ^1/_2$　插页:4
印数:1—4,029
1987年10月第1版　1987年10月第1次印刷

责任编辑:俞晓群　谭　坚　责任校对:王淑芬
封面设计:安今生　插　图:安　迪

统一书号:7371·501　定价:1.35元
ISBN 7-5382-0174-2

内 容 简 介

本书是"世界数学名题欣赏丛书"之一。所谓希尔伯特第十问题，是1900年德国数学家希尔伯特在巴黎的国际数学家大会上提出的关于"刁藩图方程解的判定问题"，也就是判定不定方程是否有解的方法问题。这一问题虽已在1970年得到否定的解决，但是在数学中产生了十分深远的影响。本书介绍了第十问题的内容和研究情况，阐述了它对于整个当代数学研究的促进作用，理论严整，论述生动。

Summary

This book is one of A Series World Famous Mathematics Appreciation. So-called Hilbert's tenth problem is the decidability problem of Diophantus solution of equations, raised by German mathematician Hilbert at International Mathematician Congress in Paris in 1900. That is the problem of deciding whether indefinite equation has solution. Though the problem was given a negative solution in1970, it has brought about a profound and lasting influence in mathematics.The book introduces the content and study situation of the tenth problem, and sets forth its promoting function to the whole research on modern mathematics. The theory is in neat formation and the exposition is vivid.

序言

1900年，德国大数学家希尔伯特在巴黎的国际数学家大会上提出了23个数学问题，揭开了二十世纪数学发展的一页，激励着有为的数学家们去思索，去探求，去拼博！而第十问题就是其中精采的一个。

人们知道，数学问题作为数学研究的对象，也是推动数学发展的动力，人们为了解决数学难题，要引入新概念，寻找新的工具，这方面的例子是不少的。

关于解一个特定的刁藩图方程本是一个古老的数学问题，某些两个变元的二次方程人们早就发现了它们的解法，而对两变元的三，四次刁藩图方程并未发现一般的解的方法，对特定的一个这样的刁藩图方程，证明它是否有解，或当有解时求出它们的解，也不是一件容易的事。

然而，在本世纪六十年代末，英国数学家贝克成功地对一类两变元刁藩图方程给出了一个有效的方法，可求出它们的一切解，他成功地确定

了一个仅依赖于次数n及多项式系数的上界B，使对任意解(x_0,y_0)有：

$$\max(|x_0|,|y_0|)\leqslant B$$

由于贝克的这一出色工作，他获得了1970年的菲尔兹奖。

希氏第十问题的解决是集体的智慧，使人惊奇的是只用了一点数理逻辑和初等数论就解决了这一世界大难题。美国数学家戴维斯，鲁宾逊和普特南作出了突出的贡献，而最终的一步是在1970年由苏联青年数学家马吉雅塞维奇完成的。

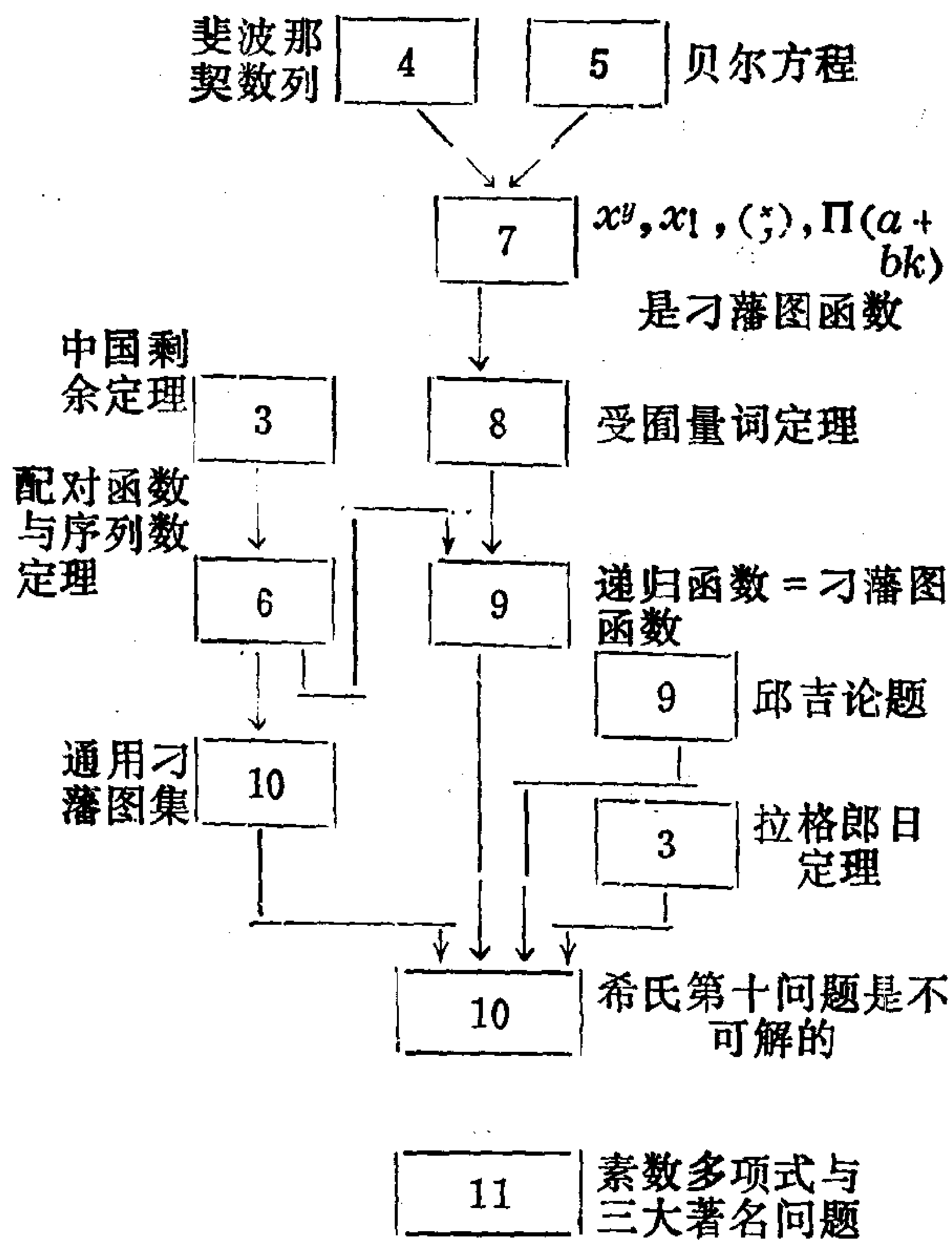
本书做为读者欣赏的一个数学问题，书中用到的知识力图自封，它不需要读者有什么特殊的数学修养。为了便于读者阅读，我们还给了一个全书内容的联系图，以供参考。

在本书的写作过程中，曾和北京大学吴允曾教授多次交谈，并得到中国科学院软件所研究员杨东屏老师及南开大学徐书润副教授的帮助，趁此深深表示感谢。

由于水平所限，书中缺点和错误望读者指正。

胡久稔

1987年2月



本书内容逻辑联系图（图中数字为章号）

5

01-51
1:4



作 者 简 介

胡久稔，1939年2月生，河北省雄县人。1963年7月毕业于中国科学技术大学应用数学系应用数学专业，分配在中国科学院沈阳计算技术研究所工作。二十多年来，参加了多台计算机的设计，在《数学通报》、《数学的实践与认识》上发表论文三篇，编著书《数学趣题与BASIC 程序》。现为南开大学数学研究所副研究员，从事计算机科学、数理逻辑的研究与教学工作。

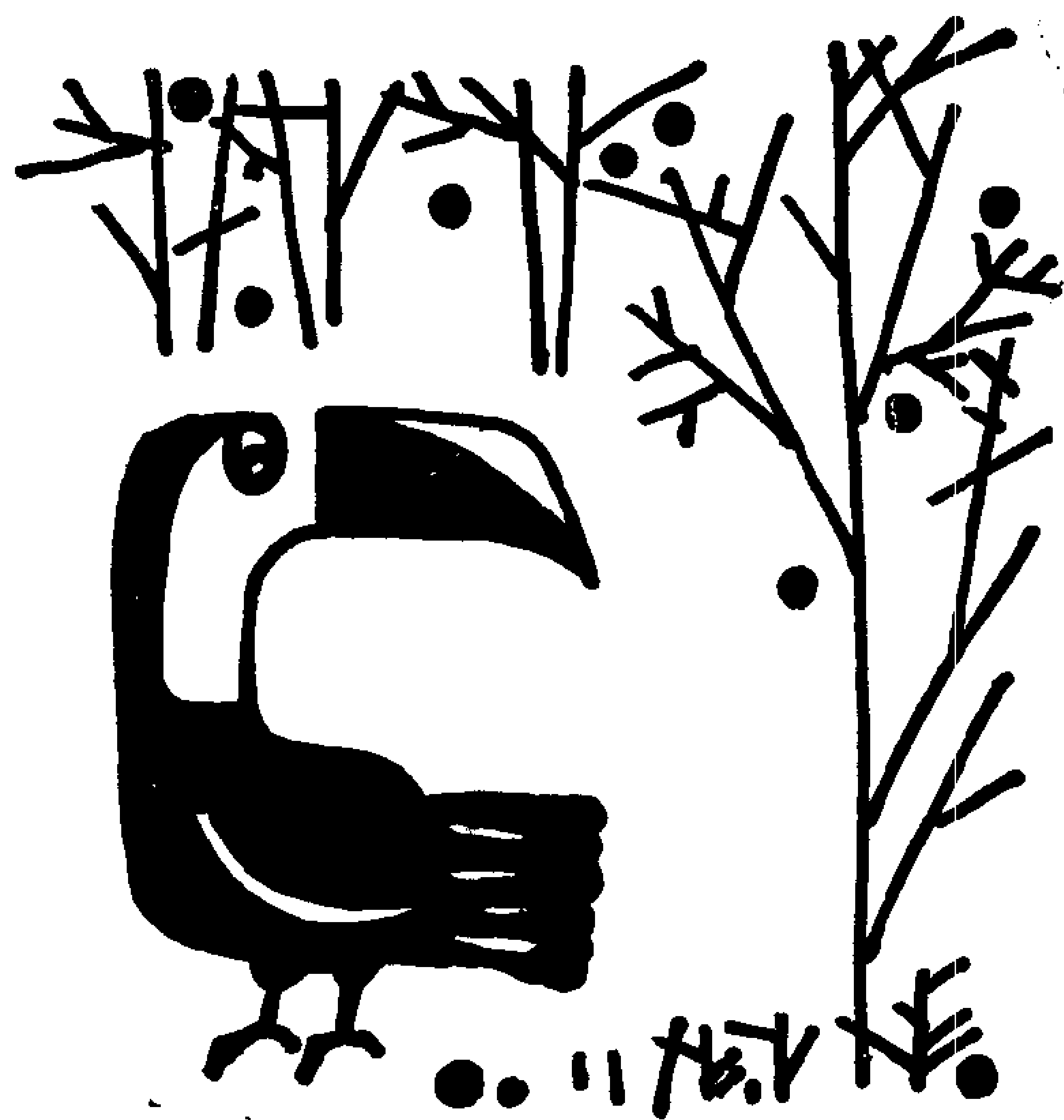
世界数学名题欣赏丛书

费马猜想
黎曼猜想
连续统假设
希尔伯特第十问题
欧几里得第五公设
哥德尔不完全性定理
不动点定理
无处可微的连续函数
科克曼女生问题
斐波那契数列
哥德巴赫猜想
置换多项式及其应用
素数判定与大数分解
货郎担问题

目 录

Contents

一　希尔伯特第十问题的提出



我们都知道，从古希腊时代，人们就对不定方程的整数解感兴趣，人们先从一个几何学上的定理：一个直角三角形，站在两直角边上的正方形的面积之和恰等于站在斜边上的正方形的面积。这就是毕达格拉斯定理，又称商高定理。

上述定理用代数的语言说是方便而直观的，即令 a,b为直角三角形的两直角边，c 为斜边，则

$$a^2+b^2=c^2$$

人们自然想到，变元 x,y,z 取正整数的不定方程：

$$x^2+y^2=z^2 \qquad (1)$$

它的解本身就包含有美的享受，而且是毕氏几何定理的“数”的体现。人们对（1）的整数解的直观概念可追溯得更早，古巴比伦人在公元前两千多年就发现了3，4，5是它的一组解，并聪慧地用绳索分别3，4，5等分再对折以制造出一个直角（如图1.1），这对测量土地是十分必要的。

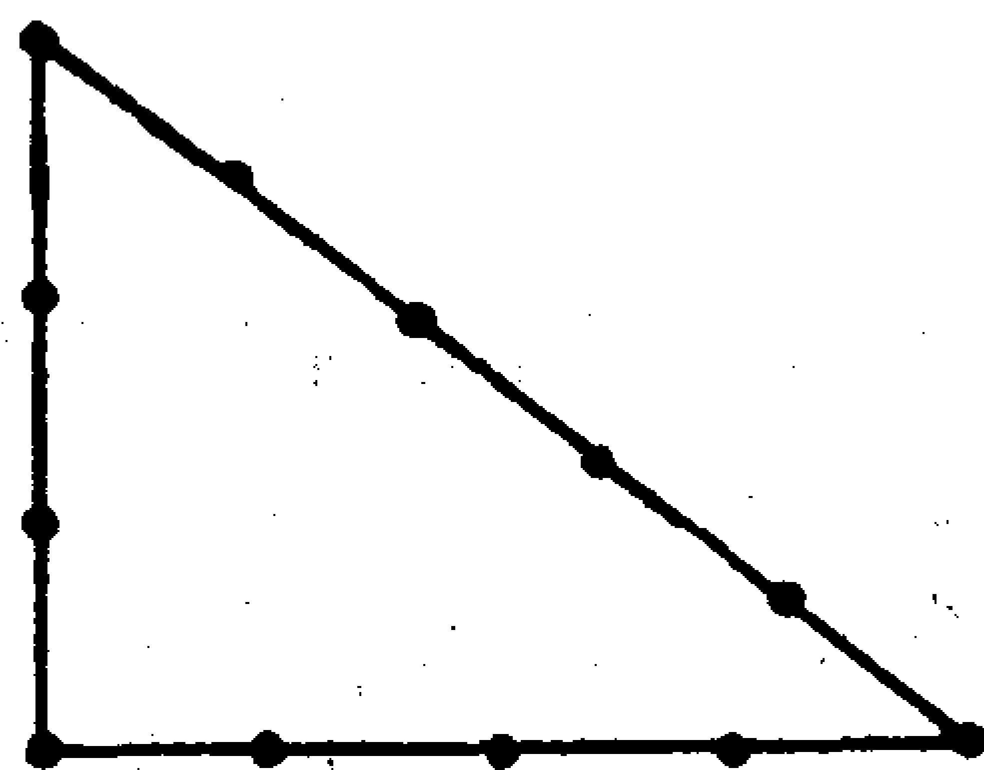


图1.1

方程（1）的一个解（3，4，5），我国商高也早已发现，在两千年前的一部数学著作《周髀算经》中有记载，而后，在我国另一本名著《九章算术》中又列出了几组解：

(5,12,13)

(7,24,25)

(8,15,17)

(20,21,29)

在古希腊，毕达格拉斯学派发现，当 m 是奇数时，$\left(m,\ \frac{1}{2}(m^2-1),\ \frac{1}{2}(m^2+1)\right)$是方程(1)的一组解，但在那个时代，都没能给出（1）的完全的整数解。

到了公元三世纪，有一位著名的希腊数学家

叫刁藩图（约公元246—330），在他写的一本《算术》书中，最先讨论了方程（1）的整数解，他得出：

$$x=2mn$$
$$y=m^2-n^2$$
$$z=m^2+n^2$$

其中 m,n 互素，$m>n$

到了十七世纪，刁藩图的书为法国数学家费马所注意，他深入地研究了这类方程（以后我们称之为刁藩图方程），并得到一个为后世所惊奇的定理：

方程 $x^n+y^n=z^n$

当 $n>2$时，无非零的正整数解。

自然，这是一个特殊的刁藩图方程，费马自称已证明了这一定理，但后人并未发现他的证明，不但如此，在近二百多年来，无数数学家经过艰辛地拼搏，也未能完全解决它，即既不能证明它，又不能举出一个反例而推翻它。于是，人们已把它称之为费马猜想或费马大定理。关于这一问题的最好结果是由德国数学家法尔廷斯给出的，他指出，如果这一刁藩图方程有解，则只有有限多个解，这自然已是一惊人的突破，他把人们在茫茫无限中的考虑变成有限中的论证。

到了二十世纪初，一位著名的德国数学家希

尔伯特，在1900年于巴黎召开的国际数学大会上，他总结而提出了二十三个数学问题，提醒数学家们要搞清楚这些问题，他没有把费马猜想做为一个问题提出，而把比它更广的所谓刁藩图方程的可解性做为第十个问题而列出，他说：

“10．任意刁藩图方程的判定。

设给了一个具有任意多个未知数的整系数刁藩图方程，要求给出一个方法（verfahren），使得借助于它，通过有穷次运算可以判定该方程有无整数解。”

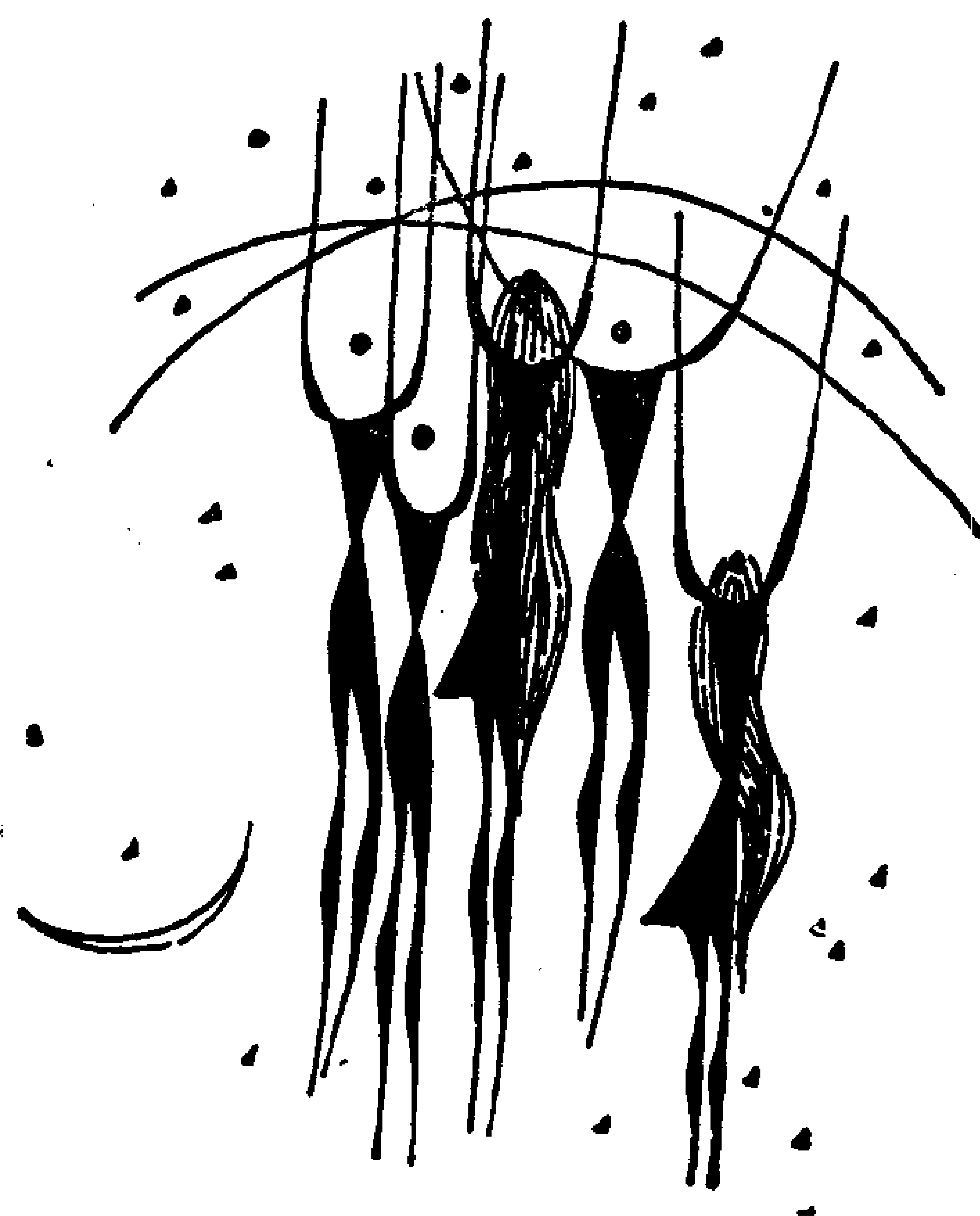
这里的方法（verfahren）就是英文的算法（algorithm），而算法的概念对我们是并不陌生的，其实这个词是很古老的，远在古希腊时代，人们就知道如何求两个数的最大公约数，这就是欧几里德算法，又称辗转相除法。还有，如任给一个自然数判定它是否是一个素数，也存在着一个方法（算法），这就是筛法．称埃拉托斯散筛法，这就是说，任给一个自然数，在有限步内总能通过这一筛子，以判定这个数是已被筛掉还是在筛子里。

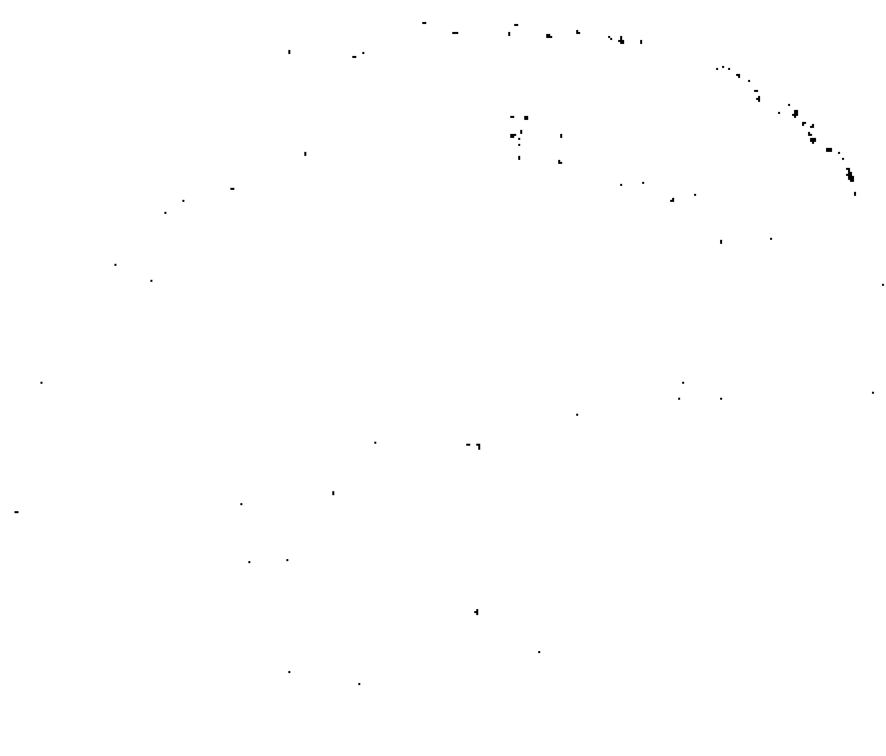
虽然，人们很早就有了算法的朴素的概念，但在本世纪三十年代以前，对算法概念是不精确的，人们只是把用以能行地解决一类相似问题的方法叫做算法，而所谓“能行”是指按照一定的

规则，能在有穷步中机械地得到结果。

希尔伯特第十问题问世以来，人们尚未给算法以精确化，数学问题的可解与不可解究竟是什么含意人们还不得而知，人们在一片黑暗中度过这三十年的岁月，企图寻找这一问题有算法的数学家们都一个个碰壁，第十问题毫无进展，我们后来才明白，这时解决这一问题的时机尚不成熟，人们面对着困难，在思索，在前进，这就促进了数学的发展！

二　数理逻辑有关基础知识






图书专用章

为了读者阅读方便，我们对后面的一些章节中会用到的某些逻辑知识加以介绍，我们不去很严格地论述，只是为以后作准备。

1. 命题及其联结词

（一）命题．什么是命题呢？在日常生活中，我们常常说一些具有判断的句子，这样表示判断的句子就称为命题。

命题是有真假的，在我们以后的讨论中，命题只取真假两个值．我们一般用T表示真值，用F表示假值，有时为了直观和应用的方便，用“1”表示真值，用“0”表示假值。

下面我们举些例子，说明命题及其真假。

（1）$1+2\neq3$。

（2）月亮从西方升起。

（3）$x+y=5$.

（4）小林光一是日本的棋圣。

（5）2000年，一个战胜世界象棋冠军的计

算机程序会出现。

（6）希尔伯特是法国人。

我们看到，（1）是个命题，它取假值F，（2）也是一个命题，也取值为F，（3）不是一个命题，因为变量x，y以不同的值代入，它有时取真值，有时取假值。（4）是一个真命题，因为当今日本的围棋棋圣是小林光一，过些时候，如果棋圣易人，则该命题取假值。（5）是一个命题，但现在尚不能知道它是真还是假的，可是，到2000年就会给出真或者假的判定。（6）是一个命题，它取假值，因为希尔伯特是德国人。

上面都是一些简单形式的命题（除了(3)），还有一些很难判断真假的命题，因而成为大难题，如：

（7）一个大偶数总可表示成两个素数之和（哥德巴赫猜想）。

（8）斐波那契数列中有无限多个素数。

它们都是命题，但人们还不知其真假。

（二）命题联结词。

令P,Q是两个命题，则用$\neg$（非，还用$-$，$\sim$表示），$\wedge$（与，还用&表示），$\vee$（或），$\longrightarrow$（蕴涵），$\longleftrightarrow$（等值）联结词可产生如下新的命题：

$\neg P$，$P\wedge Q(P\& Q)$，$P\vee Q$，$P\rightarrow Q$，$P\longleftrightarrow Q$，它们的含意是这样的：

$\neg P$，当 P 为真时，$\neg P$ 为假，P 为假时，$\neg P$为真。

$P\wedge Q$，只当 P 与Q都是真时才为真，否则为假，符号$\wedge$的其他通用符号是“&”，“·”.

$P\vee Q$，P 或者 Q 有一个真则$P\vee Q$ 为真，否则为假，符号$\vee$常用“+”来替代。

$P\longrightarrow Q$，它称为蕴函式，$P\longrightarrow Q$为真，只当P为假或者 Q 为真。这里 P称为蕴涵式的前件，Q称为其后件．常用的蕴涵符号还有“$\supset$”。

$P\longleftrightarrow Q$，它取值为真，当 P,Q 取相同的真值或假值，事实上，$P\longleftrightarrow Q$和$(P\longrightarrow Q)\wedge(Q\longrightarrow P)$ 取相同的值，这一点下面还会说明。

自然，命题联结词还有一些，上面这些是最常用的，例如舍弗提出的舍弗“|”，是一个重要而有用的联结词，在计算机的 MOS 电路中，大量地应用这一元件，舍弗“|”的定义是：

$$P|Q=\neg(P\wedge Q)$$

2. 命题形式的变换

象初等代数中的某些代数式间的恒等变换，在命题逻辑中也是同样发生的，命题演算的本质

就是要象代数的式子，方便地进行恒等变换。例如，在代数中，有

$$x^2+2xy+y^2=(x+y)^2$$

$$\sqrt{x^2}=|x|$$

$$x^2-y^2=(x+y)(x-y)$$

等，这里代数恒等式的含意是，对 x，y 的任意代入（自然要预先给定一个数域），等号的左边的值和右边的值相等。

由于命题变量只取真、假值，所以，我们对基本的命题联结词及其更复杂的表达式可以用赋值的方法，“计算”出它们的值（T 或者 F），这称为真值表。用这种方法，列出下列命题联结词的真值表是十分清楚的：

P	$\neg P$
T	F
F	T

P	Q	$P\wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

P	Q	$P\vee Q$
T	T	T
T	F	T
F	T	T
F	F	F

P	Q	$P\to Q$
T	T	T
T	F	F
F	T	T
F	F	T

P	Q	$P\leftrightarrow Q$
T	T	T
T	F	F
F	T	F
F	F	T

我们给出舍弗“|”及另一个模“2”和的真值表，后者是计算机运算功能最基本的“细胞’，模“2”和是如下定义的：

$$P\oplus Q=\neg(P\leftrightarrow Q)$$

不难用真值表验证：

$$P\oplus Q=(\neg P\wedge Q)\vee(P\wedge\neg Q)^{*}$$

P	Q	$P\mid Q$
T	T	F
T	F	T
F	T	T
F	F	T

P	Q	$P\oplus Q$
T	T	F
T	F	T
F	T	T
F	F	F

我们可以利用真值表证明逻辑表达式间是否相等，即证明命题表达式间是否等价。

例 试证明：

（1）$P\to Q=\neg P\vee Q$

（2）$P\to(Q\to R)=(P\wedge Q)\to R$

---

* 我们一般可定义运算符的优先次序为：$\neg,\wedge,\vee$，这样可省略括号为$\neg P\wedge Q\vee P\wedge\neg Q$.

（1）、（2）对应下面两个真值表：

P	Q	$P\to Q$	$\neg P\vee Q$
T	T	T	T
T	F	F	F
F	T	T	T
F	F	T	T

P	Q	R	$P\wedge Q$	$(P\wedge Q)\to R$	$Q\to R$	$P\to(Q\to R)$
T	T	T	T	T	T	T
T	T	F	T	F	F	F
T	F	T	F	T	T	T
T	F	F	F	T	T	T
F	T	T	F	T	T	T
F	T	F	F	T	F	T
F	F	T	F	T	T	T
F	F	F	F	T	T	T

从上表看出，$P\to Q$一列的值与$\neg P\vee Q$一列的值是完全相同的，这就证明了$P\to Q$与$\neg P\vee Q$是相等（等价）的。而$(P\wedge Q)\to R$一列下的值与$P\to(Q\to R)$一列下的值是一样的，从而证明了$P\to(Q\to R)$等于$(P\wedge Q)\to R$。

命题表达式的形式可以是多种多样的，从等值的观点上看，它可以从一种形式变成另一种形式，这种变换是很有用的，在计算机及其他自动

系统的设计中，它是逻辑网络综合必不可少的一个工具。

命题形式的变换还可通过下面的等式进行，如果我们以“+”表示“∨”，以“·”（或省略“·”号）表示“∧”，以“—”表示“┐”。于是有：

1° $A \cdot A = A$

2° $A + A = A$

3° $A(BC) = (AB)C$

4° $A + (B + C) = (A + B) + C$

5° $AB = BA$

6° $A + B = B + A$

7° $AB + C = (A + C)(B + C)$

8° $(A + B)C = AC + BC$

9° $\overline{\overline{A}} = A$

10° $\overline{AB} = \overline{A} + \overline{B}$

11° $\overline{A + B} = \overline{A}\,\overline{B}$

12° $A \cdot T = A$

13° $A \cdot F = F$

14° $A + F = A$

15° $A + T = T$

16° $A + (AB) = A$

17° $A(A + B) = A$

公式10°，11°是很重要的，又，对⟶，⟷可通过下述公式而为∧，∨，┐表示，

$$P\leftrightarrow Q = (P\rightarrow Q)\wedge \underline{(Q\rightarrow P)}$$

$$P\rightarrow Q = \neg P\vee Q = P\wedge\overline{Q}$$

3. 个体词、谓词与量词

在命题演算中，我们把简单命题认为是不可分的，只研究简单命题和用联结词构成的复合命题的逻辑关系和推理关系，然而，我们发现有些推理关系用命题逻辑是很难表示的，一个著名的例子是所谓苏格拉底论断：

P：所有的人都是要死的。

Q：苏格拉底是人。

R：苏格拉底是要死的。

从命题逻辑的角度看，这三句话都是命题，然而，它们显然有着密的关系，即，如果前两个命题是真的，可以自然的推出第三个命题也是真的，可写成推理图示：

$$\begin{array}{c} P \\ Q \\ \hline R \end{array}$$

或表示为 $(P\&Q)\rightarrow R$，但这一复合命题在命题逻辑中并非永真公式。从而看出，有必要对简单命题作进一步分析，深入分析命题中的内部结构，于是引进了谓词的概念，而这种以命题中谓词为

基础的分析研究，称之为谓词演算。

（一）个体词、谓词

命题：7是一个素数，这句话里，显然“7”是主语，而“是一个素数”是谓语，这一命题表示了主语（7）所具有的属性（是一个素数），这“…是素数”是一个谓语。

在数理逻辑中，将命题里表示思维对象的词称作个体词，而将表示一个个体的性质和两个或两个以上个体之间关系的词称作为谓词。我们令 $x_1, x_2, \cdots, x_n$ 表示变量（或个体变量），它取值的集合称为个体域或论域，于是我们称谓词 $P(x_1, \cdots, x_n)$ 为 n 元（目）谓词，而对具体的个体词 $a_1, \cdots, a_n$，则 $P(a_1, \cdots, a_n)$ 是一个命题，它可取真或假的值。

在以后各章中，我们讨论的是数论谓词 $P(x_1, \cdots, x_k)$，即变元取自自然数*，当对 $x_1, \cdots, x_k$ 赋值后，谓词 P 变成一个命题，它可取真（以“1”表示）或假（以“0”表示）两个值，从而，有时我们也称 $P(x_1, \cdots, x_k)$ 为一谓词函数，它只取“0”，“1”两个值。

于是，令 P_r 表示谓词“…是素数”，于是

---

* 自然数集在数学中定义为集合$\{1, 2, 3, \cdots\}$，而在逻辑或递归函数中，往往扩充为$\{0, 1, 2, \cdots\}$，这一点不是本质中。有时我们也不加说明。

命题："7是一个素数"，可表示为$P_r(7)$，显然，它是一个真命题。

（二）量词

命题里表示数量的词称为量词，在谓词演算中，常见的有三种量词：

（1）全称量词$\forall$，表示的含意是"所有"，"凡是"，"全部"等等。

例如，给定一个论域D，对一元谓词$P(x)$而言，$(\forall x)P(x)$，是说，对所有D中元素a，$P(a)$都真。自然，能否有$(\forall x)P(x)$，这除了和谓词P有关，还和x的变化范围即论域D有关。如，$(\forall x)(x^2=x)$，在论域$D=\{0,1\}$中成立，而在D为自然数集时，不能有$(\forall x)(x^2=x)$，自然也不能有$(\forall x)(x^2\neq x)$。

（2）存在量词$\exists$，表示的含意是"存在"，"有"，"至少有一个"等等。

（3）存在唯一量词$\exists!$，它表示存在且只存在唯一的一个。

例1　存在着偶素数。

令$E(x)$表示x是偶数，$P_r(x)$表示x是素数，则该命题表示为：

$$(\exists x)[E(x)\&P_r(x)]$$

由于"2"是唯一的偶素数，所以形式化命题：存在着唯一的一个偶素数为

$$(\exists ! x)(E(x) \& P_r(x))$$

例 2 方程 $x^2-3y^2=1$有正整数解。

该命题形式化为：

$$(\exists x)(\exists y)(x^2-3y^2=1)$$

x,y 的论域是集合 $D=\{1,2,3,\cdots\}$。

例 3 素数是无穷的。（欧几里得）

该命题可形式化为：

$$(\forall x)(\exists y)(y>x \& P_r(y))$$

即，任给一个自然数 x，总存在一个 y，y 大于 x 且y 是素数。

4．谓词演算的推理规则

在后面的论述中，我们有时自觉或不觉的使用了下面的推理规则，在这之前，先解释几个术语。

公式 $(\forall x)(P(x,y))\&Q(x,y)$

（其中 $P(x,y)$ 中的 x 标为“约束变元”，$Q(x,y)$ 中的 x 标为“自由变元”）

在量词（$\forall x$或 $\exists x$，$\exists ! x$)作用下的变元称为约束变元，否则称自由变元，它们在公式中的出现，相应的叫做约束（或自由）出现。上面公式中，x 有一约束变元，有一自由变元，而y 均是自由变元。

（一）全称量词消去

$$\frac{(\forall x)A(x)}{A(y)}$$

这里，横线上为前提，横线下为结论，而 $A(x)$ 为任意一个含有x自由出现的命题形式，$A(y)$ 是将$A(x)$中的x处处代之以y，要求y在$A(x)$中不约束出现。自然，对x论域中的任一a，$A(a)$均成立。

该规则的意思是：如果x论域中的所有元素都是性质A，则论域中的任一元素也有性质A。

（二）全称量词的引入

$$\frac{A(y)}{(\forall x)A(x)}$$

这规则的含意是，如果对论域中任一个体都具有性质A，则对个体域的全体个体都有性质A。注意，这里y必须是自由变元，并且x不出现在$A(y)$中。

（三）存在量词的消去

$$\frac{(\exists x)A(x)}{A(a)}$$

这里a是x论域中一个确定的一个体项，但a不出现在$A(x)$中。

（四）存在量词的引入

$$\frac{A(a)}{(\exists x)A(x)}$$

这里只要求 x不在 $A(a)$中出现。

5. 前束范式定理

谓词公式 $A=B$，如果对其中所有的命题给所有可能的真假值代入，对所有个体变量取某论域的任何元素，A,B 有相同的真假值．此时，称A与 B等值。用另一种方式说，当 A 对某一赋值为真时，则 B对相同的赋值亦真，反之，对 B 的某一赋值为真，则 A 对这一赋值也为真。

定义2.1 公式 A具有形式

$(Q_1x_1)\cdots(Q_nx_n)B$，其中(Q_ix_i)或为$(\forall x_i)$，或为 $(\exists x_i)$，$x_1,\cdots,x_n$ 均为相异变元，B 中不含量词，则称 $(Q_1x_1)\cdots(Q_nx_n)B$为 A的前束范式。

下面的一些等值公式是容易用前述的推理规则加以证明的。

（一）若公式 A 不含自由变元x，则

$$(\forall x)A=A \qquad (1)$$

$$(\exists x)A=A \qquad (2)$$

（二）全称量词和存在量词的转换

$$\neg(\forall x)A(x)=(\exists x)(\neg A(x)) \qquad (3)$$

$$\neg(\exists x)A(x) = (\forall x)(\neg A(x)) \quad (4)$$

（三）若A不包含自由变元x，则

$$A \wedge (Qx)B(x) = (Qx)(A \wedge B(x)) \quad (5)$$

$$A \vee (Qx)B(x) = (Qx)(A \vee B(x)) \quad (6)$$

（四）对公式 A, B有：

$$(\forall x)A(x) \wedge (\forall x)B(x) = (\forall x)(A(x) \wedge B(x)) \quad (7)$$

$$(\exists x)A(x) \vee (\exists x)B(x) = (\exists x)(A(x) \vee B(x)) \quad (8)$$

（五）对不同约束变元的等值式：

$$(Q_1x)A(x) \wedge (Q_2y)B(y) = (Q_1x)(Q_2y)(A(x) \wedge B(y)) \quad (9)$$

$$(Q_1x)A(x) \vee (Q_2y)B(y) = (Q_1x)(Q_2y)(A(x) \vee B(y)) \quad (10)$$

再注意我们曾证明过的等值式：

$$A \rightarrow B = \neg A \vee B \quad (11)$$

$$A \leftrightarrow B = (A \rightarrow B) \wedge (B \rightarrow A) = (\neg A \vee B) \wedge (A \vee \neg B) \quad (12)$$

$$A \leftrightarrow B = (A \wedge B) \vee (\neg A \wedge \neg B) \quad (13)$$

$$\neg\neg A = A \quad (14)$$

$$\neg(A \wedge B) = \neg A \vee \neg B \quad (15)$$

$$\neg(A \vee B) = \neg A \wedge \neg B \quad (16)$$

于是有定理。

定理2.1 （前束范式定理）

任一谓词公式，总存在着与它等值的前束范式。

证 我们可通过以下各步，使量词逐步都放置于前面。假定给了公式A。

1° 将 A 中某些变量改名，以为我们使用（9），（10）式。

2° 用$\wedge$，$\vee$，$\neg$运算，消去$\longrightarrow$和$\longleftrightarrow$。

3° 通过（3），（4）、(14)、（15）、（16）可将“$\neg$”加在原子公式上。

4° 通过（5）——（10）将量词都放在整个公式的左端。 □

例 设

$$A=\neg[(\forall x)(\exists y)F(a,x,y)\rightarrow(\exists x)[\neg(\forall y)G(y,b)\rightarrow H(x)]]$$

变换可由以下几步：

$$A=\neg\neg[(\forall x)(\exists y)F(a,x,y)\vee(\exists x)[\neg\neg(\forall y)G(y,b)\vee H(x)]]$$

$$=(\forall x)(\exists y)F(a,x,y)\wedge\neg(\exists x)[(\forall y)G(y,b)\vee H(x)]$$

$$=(\forall x)(\exists y)F(a,x,y)\wedge(\forall x)\neg[(\forall y)G(y,b)\vee H(x)]$$

$$=(\forall x)(\exists y)F(a,x,y)\wedge(\forall x)[\neg(\forall y)G(y,b)\wedge\neg H(x)]$$

$$=(\forall x)(\exists y)F(a,x,y)\wedge(\forall x)(\exists y)$$

$$[\neg G(y,b) \wedge \neg H(x)]$$

$$= (\forall x)[(\exists y)F(a,x,y) \wedge (\exists y)$$

$$[\neg G(y,b) \wedge \neg H(x)]$$

$$= (\forall x)[(\exists y)F(a,x,y) \wedge (\exists z)$$

$$[\neg G(z,b) \wedge \neg H(x)]$$

$$= (\forall x)(\exists y)(\exists z)[F(a,x,y)$$

$$\wedge \neg G(z,b) \wedge \neg H(x)]$$

得到的前束范式 B为：

$$B = (\forall x)(\exists y)(\exists z)[F(a,x,y) \wedge \neg G(z,b)$$

$$\wedge \neg H(x)]$$

三　中国剩余定理与拉格郎日定理



在以后的论证中我们需要数论中的两个重要的定理，一是中国剩余定理，它在递归函数的某些证明技巧中是很有用的，著名已故数学家哥德尔最先使用了中国剩余定理。

拉格郎日定理是说任一自然数可表为四个整数的平方和，由于这一定理在希尔伯特第十问题上的应用，这一“古老”的定理似乎焕发了青春。

1．中国剩余定理

关于解联立一次同余式的问题，我国古代的研究有着光辉的一页，早在《孙子算经》一书中（纪元前后），曾提出并解决了下列问题：

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何．答曰二十三，……”

书中给出了解法，用现代初等数论的表示法是：

解联立同余式：

$$X\equiv 2 \pmod 3$$

$$X\equiv 3 \pmod 5$$

$$X\equiv 2 \pmod 7$$

其解法是：若一数用 3 除余 a，用 5 除余 b，用 7 除余 c，则此数是：

$$X\equiv 70a+21b+15c \pmod{105}$$

关于这一解法在明朝程大位的《算法统宗》一书中有一首歌谣：

三人同行七十稀
五树梅花廿一枝
七子团圆整半月
除百零五便得知

它形象而生动地描述了这一求解算法。

孙子以后，许多中国数学家把孙子的问题进一步推广，总结出中外驰名的中国剩余定理。

定理 （中国剩余定理）

令 $a_1,a_2,\cdots,a_n$ 是任意的正整数，且令$m_1,m_2,\cdots,m_n$ 是两两互素的一个序列，那么一定存在着一个这样的 X，

$$\begin{cases} X\equiv a_1 \pmod{m_1} \\ X\equiv a_2 \pmod{m_2} \\ \vdots \\ X\equiv a_n \pmod{m_n} \end{cases} \qquad (1)$$

证

令 $m_1m_2\cdots m_n=M$

$$M_j=M/m_j \quad (j=1,2,\cdots,n)$$

则 $(M_j,m_j)=1 \quad (j=1,2,\cdots,n)$

所以必有n个数 $a_1,a_2,\cdots,a_n$使得

$$M_ka_k\equiv 1 \pmod{m_k} \quad (k=1,2,\cdots,n)$$

又若 $l\neq k$，$m_l|M_k$

$$\therefore M_ka_k\equiv 0 \pmod{m_l},\ l\neq k$$

故令

$$R=\sum_{i=1}^{n}M_ia_ia_i$$

则

$$R\equiv M_1a_1a_1\equiv a_1 \pmod{m_1}$$
$$R\equiv M_2a_2a_2\equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$R\equiv M_na_na_n\equiv a_n \pmod{m_n}$$

$\therefore$ R 是满足（1）中 n 个同余式的一个解。 □

显然，解x 可以假定为正整数，这是因为，对任意一个解y，$y+kM$ $(k=0,1,2,\cdots)$ 仍然是一个解。

又，令$r_m(x,y)$表示 x被 y除的余数，于是上述的联立同余式还可写为：

$$r_m(x,m_i)=a_i \quad (i=1,2,\cdots,n)$$

2. 拉格郎日定理

拉格郎日定理是回答这样一个问题：

一个自然数可用几个整数的平方和表示呢？即，我们对任一自然数，最少用下面集合中的几个元素之和表示呢？这个集合S是：

$$S=\{0,1,4,9,\cdots,k^2,\cdots\}$$

类似的问题古代数学家们也是有兴趣的，比如，对于形如

$$T_k=\frac{k(k+1)}{2}\quad(k=1,2,\cdots)$$

的数称为三角数，人们也问，任一自然数可以用诸三角数的和表示吗？如可以，最少需要几个？

这个有趣的问题是被费马解决的，费马证明了：

任一自然数可用三个三角数之和来表示。顺便提一句，著名的大难题——哥德巴赫猜想不是也有相似的叙述——任一大偶数都可以表为两个素数之和。

这类数学问题，表述起来很简单，很直观，但证明起来就不容易了。

定理 （拉格郎日）

每一个自然数均可表为四个整数的平方和。

一个很容易证明的命题是：

存在着自然数，它不能表为三个整数的平方和。这只要找到一个这样的自然数即可。我们发现 7 就是一个这样的数，它的最短的表示是：

$$7=2^2+1^2+1^2+1^2$$

这说明拉格朗日定理是精确刻化了“一个自然数表为诸平方数之和”这一数学概念。

引理 每一个素数均能表为四个整数的平方和。

证 因为 $2=1^2+1^2+0+0$，故对素数 2 的情况定理成立，设素数 $p\neq 2$，先证明：

(i) 存在着整数 x, y, m 使得下面的表示式成立：

$$1+x^2+y^2=mp,\quad 0<m<p$$

考虑下列 $p+1$ 个整数

$$0^2, 1^2, 2^2, \cdots, \left(\frac{p-1}{2}\right)^2,\quad -1,\quad -1-1^2,$$

$$-1-2^2, \cdots, -1-\left(\frac{p-1}{2}\right)^2$$

因为对模 p 来说只有 p 个剩余，故有两个整数 x, y 存在，使得

$$x^2\equiv -1-y^2 \pmod p$$

$$0\leqslant x\leqslant \frac{p-1}{2}$$

$$0\leqslant y\leqslant \frac{p-1}{2}$$

因此有 $1+x^2+y^2=mp$

而 $0<1+x^2+y^2<1+2\left(\frac{p}{2}\right)^2<p^2$

故 $0<m<p$

(ii) 由(i)我们知道 p 有一个正倍数能表成四个整数的平方和，因此 p有一个最小的正倍数能表成四个整数的平方和，我们把它写成m_0p，则有：

$$m_0p=x_1^2+x_2^2+x_3^2+x_4^2,\quad 0<m_0<p \quad (*)$$

我们将证明 $m_0=1$。

首先证明m_0 是奇的。因为若不然，假定m_0为偶的，则 $x_1^2+x_2^2+x_3^2+x_4^2$ 是偶的，容易推出 $x_1+x_2+x_3+x_4$ 也是偶的，于是有三种可能的情形：

1° x_1,x_2,x_3,x_4 均为偶的

2° x_1,x_2,x_3,x_4 均为奇的

3° 有两个是偶的，有两个是奇的，不妨假定 x_1,x_2 是偶的，x_3,x_4 是奇的，但是

$$x_1+x_2,\quad x_1-x_2,\quad x_3+x_4,\quad x_3-x_4$$

总是偶的，于是有：

$$\frac{1}{2}m_0p=\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2$$

$$+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2$$

即$\frac{1}{2}m_0p$能表成四个整数的平方和，这与 m_0 的意义相矛盾，故m_0 只能是奇数。

假定 $m_0>1$,则 $m_0\geqslant 3$,且

$m_0\nmid(x_1,x_2,x_3,x_4)$，因为若不然，由(*)式 $m^2{}_0|m_0p$,因而 $m_0|p$，这与 $1<m_0<p$ 相矛盾。故存在着不全为零的四个数 y_1,y_2,y_3,y_4,使得下列式子成立：

$$y_i\equiv x_i(\bmod\ m_0),\ |y_i|<\frac{1}{2}m_0$$

$$(i=1,2,3,4)$$

因此， $0<y^2{}_1+y^2{}_2+y^2{}_3+y^2{}_4<4\left(\frac{1}{2}m_0\right)^2=m^2{}_0$

$$y^2{}_1+y^2{}_2+y^2{}_3+y^2{}_4\equiv x^2{}_1+x^2{}_2+x^2{}_3+x^2{}_4\equiv 0$$
$$(\bmod\ m_0)$$

即 $y^2{}_1+y^2{}_2+y^2{}_3+y^2{}_4=m_0m_1,\ 0<m_1<m_0$

$$\therefore\ (m_0m_1)(m_0p)=m^2{}_0m_1p$$

又，容易验证：

$$(x^2{}_1+x^2{}_2+x^2{}_3+x^2{}_4)(y^2{}_1+y^2{}_2+y^2{}_3+y^2{}_4)$$

可还表为形式$z^2{}_1+z^2{}_2+z^2{}_3+z^2{}_4$,这称之为欧拉恒等式，即：

$$(x^2{}_1+x^2{}_2+x^2{}_3+x^2{}_4)(y^2{}_1+y^2{}_2+y^2{}_3+y^2{}_4)$$
$$=z^2{}_1+z^2{}_2+z^2{}_3+z^2{}_4$$

其中：

$$z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$$

$$z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3$$

$$z_3 = x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4$$

$$z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2$$

于是有：

$$z_1 \equiv 0 \pmod{m_0}$$

$$z_2 \equiv 0 \pmod{m_0}$$

$$z_3 \equiv 0 \pmod{m_0}$$

$$z_4 \equiv 0 \pmod{m_0}$$

令 $z_i = m_0 t_i$ $(i = 1, 2, 3, 4)$，代入到 $m^2{}_0 m_1 p$ 中有：

$$m^2{}_0 m_1 p = m_0{}^2(t^2{}_1 + t^2{}_2 + t^2{}_3 + t^2{}_4)$$

$$\therefore\ m_1 p = t^2{}_1 + t^2{}_2 + t^2{}_3 + t^2{}_4$$

注意到 $0 < m_1 < m_0$，这与m_0 的假设相矛盾，故 $m_0 = 1$。 □

主要定理证明：

因 $0 = 0^2 + 0^2 + 0^2 + 0^2$，$1 = 1^2 + 0^2 + 0^2 + 0^2$，而对任一大于 1 的自然数均可分解成素数的连乘积，由欧拉恒等式及上述引理，定理得证。

有了这个定理，关于讨论一个刁藩图方程有无整数解可归结为讨论方程有无自然数解的问题，这是因为：

$$p(x_1, \cdots, x_n) = 0 \text{有自然数解} \Longleftrightarrow$$

$p(s_1^2+t_1^2+u_1^2+v_1^2,\cdots,s_n^2+t_n^2+u_n^2+v_n^2)$
$=0$ 有整数解，在以后的讨论中，我们特别关心方程，$p(x_1,\cdots,x_n)=0$ 有无正整数解的问题，如果它不存在一个算法判定有无解，自然，希氏第十问题也不存在算法。

四　斐波那契数列



在征服希氏第十问题的征途上，最终的一步是由苏联年轻的数学家马吉雅塞维奇完成的，他在1970年，年仅二十二岁，他的著名的论文是：《可枚举集是刁藩图的》〔6〕，发表在苏联科学院院报上。

马吉雅塞维奇指出，斐波那契数列有着奇妙的性质，利用它的一系列性质，终于用初等方法完成了一个重要的定理：

一个集合是递归可枚举的当且仅当它是刁藩图的。从而最终判定了希氏第十问题是递归不可解的。下面我们介绍斐波那契数。

1. 斐波那契数列

1，1，2，3，5，8，……

表示为数列 $\{u_n\}$ $(n=1,2,\cdots)$，则

$$\begin{cases} u_1=1, \quad u_2=1 \\ u_{n+2}=u_n+u_{n+1} \quad (n=1,2,\cdots) \end{cases} \tag{1}$$

称为斐波那契数列。

为了讨论方便，有时我们需要定义 $u_0=0$，这仍满足递归关系式（1），而为了看起来更方便和直观，有时我们也用 $F(n)$ 表示第 n个斐波那契数。

（一）斐波那契数列可以写出它的显式表达式，称为比内公式：

$$u_n=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

（二）容易证明下面的加法定理：

$$u_{m+n}=u_{m+1}u_n+u_mu_{n-1} \qquad (2)$$

为了证明（2）式以及下面的需要，我们证明下面一个引理：

引理 若 α 是方程

$x^2-x-1=0$ 的一个根，则

$$\alpha^n=u_n\alpha+u_{n-1}\ (n=2,3,\cdots) \qquad (3)$$

其中u_n 是第 n 个斐波那契数。

证 施归纳于n。

当$n=2$ 时，由 $\alpha^2=\alpha+1$，（3）式成立。

当$n=3$ 时，由$\alpha^3=\alpha(\alpha+1)=\alpha^2+\alpha=2\alpha+1$

$\therefore\ \alpha^3=u_3\alpha+u_2$，（3）式成立。

设 $n=k$，$n=k+1$，（3）式成立。

即 $\alpha^k=u_k\alpha+u_{k-1}$

$\alpha^{k+1}=u_{k+1}\alpha+u_k$

$$\therefore\ \alpha^k+\alpha^{k+1}=u_k\alpha+u_{k-1}+u_{k+1}\alpha+u_k$$
$$=\alpha(u_k+u_{k+1})+(u_{k-1}+u_k)$$
$$=u_{k+2}\alpha+u_{k+1}$$

又 $\alpha^{k+2}=\alpha^k\cdot\alpha^2$
$$=\alpha^k(1+\alpha)$$
$$=\alpha^k+\alpha^{k+1}$$

$$\therefore\ \alpha^{k+2}=u_{k+2}\alpha+u_{k+1}$$

于是当 $n=k+2$ 时（3）式也成立。 □

现在证明（2）式：

$$\because\ \alpha^m=u_m\alpha+u_{m-1}$$
$$\alpha^n=u_n\alpha+u_{n-1}$$
$$\alpha^{m+n}=u_{m+n}\alpha+u_{m+n-1}$$

而 $\alpha^{m+n}=\alpha^m\cdot\alpha^n$
$$=(u_m\alpha+u_{m-1})(u_n\alpha+u_{n-1})$$
$$=u_mu_n\alpha^2+(u_mu_{n-1}+u_{m-1}u_n)\alpha+u_{m-1}u_{n-1}$$
$$=(u_mu_n+u_mu_{n-1}+u_{m-1}u_n)\alpha+u_mu_n+u_{m-1}u_{n-1}$$

$$\therefore\ u_{m+n}\alpha+u_{m+n-1}=(u_mu_n+u_mu_{n-1}+u_{m-1}u_n)\alpha+u_mu_n+u_{m-1}u_{n-1}$$

比较等式两端并注意 α的无理性有：

$$u_{m+n}=u_mu_n+u_mu_{n-1}+u_{m-1}u_n$$
$$=u_mu_{n-1}+u_n(u_m+u_{m-1})$$
$$=u_mu_{n-1}+u_{m+1}u_n$$ □

（三）两个相邻斐波那契数的平方和仍是一个斐波那契数。

从（2）式容易导出：

$$u_{2k-1}=u^2_k+u^2_{k-1}$$

在（2）中，令 $m=k-1$，$n=k$即得出。

（四）斐波那契数的倒数表达式。

我们发现关于斐波那契数的一个美妙的倒数表达式，而它的证明并不困难：

若k 为偶数，则

$$\frac{1}{u_k}=\frac{1}{u_{k+1}}+\frac{1}{u_{k+2}}+\frac{1}{u_k u_{k+1} u_{k+2}} \quad (4)$$

证

对（4）式经变换可成下式：

$$u_{k+1}u_{k-1}-u^2_k=1 \quad (*)$$

为证明（*）式，施归纳于 k。

当 $k=2$时，容易验证（*)式是正确的。

若 $k=2l$ 时（$l=1,2,\cdots$），(*）式成立，即

$$u_{2l+1}u_{2l-1}-u^2_{2l}=1$$

则当 $k=2l+2$时有：

$$u_{2l+3}u_{2l+1}-u^2_{2l+2}$$

$$=(u_{2l+2}+u_{2l+1})u_{2l+1}-u^2_{2l+2}$$

$$=u_{2l+2}u_{2l+1}+u^2_{2l+1}-u^2_{2l+2}$$

$$=u^2_{2l+1}-u_{2l+2}u_{2l}$$

$$=u^2_{2l+1}-u_{2l+1}u_{2l}-u^2_{2l}$$

$$=u^2_{2l+1}-u_{2l+1}u_{2l}+(1-u_{2l+1}u_{2l-1})$$
$$=u_{2l+1}(u_{2l+1}-u_{2l-1})-u_{2l+1}u_{2l}+1$$
$$=u_{2l+1}u_{2l}-u_{2l+1}u_{2l}+1$$
$$=1$$

从而对 $k=2l+2$时命题也成立。 □

（五）斐波那契数的界。

从（一）中，我们看到斐波那契数是一种具有幂增长速度，然而容易证明下面的命题：

（1）$u_{2k+2}\geqslant 2^k$ （5）

（2）$u_{2k}<3^k$ （6）

证 （5）式用归纳法是容易的．对于（6），用归纳法时注意偶角标斐波那契数的递归表达式：

$$u_{2k+4}=3u_{2k+2}-u_{2k}$$

而这表达式本身的正确性更是容易验证的。

2．斐波那契数的可除性

首先我们证明：

（一）若 $d|k$,则 $u_d|u_k$。

我们给出（一）的一个构造性证明，即给出商的显式表达式而不是存在性证明。

定理 若 $k=dr$ (k,d,r 为正整数,d,r 不是1），则

$$\frac{u_k}{u_d}=\sum_{i=0}^{r-1}c_i^r u_d^{r-(i+1)}u^i_{d-1}u_{r-i} \qquad (7)$$

证 由（3）式有：

$$a^k=u_ka+u_{k-1}$$

$$a^d=u_da+u_{d-1}$$

$$a^{dr}=(u_da+u_{d-1})^r$$

$$=u_d^r a^r+c_1^r(u_da)^{r-1}u_{d-1}$$

$$+c^r_2(u_da)^{r-2}u^2_{d-1}+\cdots$$

$$+c^r_i(u_dd)^{r-i}u^i_{d-1}+\cdots+u^r_{d-1} \qquad (8)$$

由 $c^r_iu_d^{r-i}u^i_{d-1}a^{r-i}$

$$=c^r_iu_d^{r-i}u^i_{d-1}(u_{r-i}a+u_{r-i-1})$$

$$=c^r_iu_d^{r-i}u^i_{d-1}u_{r-i}a+c_i^ru_d^{r-i}u^i_{d-1}u_{r-i-1}$$

又 $\because$ $a^{dr}=a^k=u_ka+u_{k-1}$ （9）

由a 的无理性以及比较（8），（9）中a 的系数有：

$$u_k=\sum_{i=0}^{r-1}c_i^ru_d^{r-i}u^i_{d-1}u_{r-i}$$

$$\therefore \frac{u_k}{u_d}=\sum_{i=0}^{r-1}c_i^ru_d^{r-(i+1)}u^i_{d-1}u_{r-i} \qquad \square$$

（二）若 $u_d|u_k$ 且 $d\neq2$,则 $d|k$。

证 对 $d=1$,是不证自明的，今令 $d\geqslant3$,若 $u_d|u_k$ 而 $d\nmid k$,则 k 可表示为：

$$k=qd+r,\text{其中 } 0<r<d$$

利用（2）式的加法定理可得出：

$$u_k = u_{qd}u_r + u_{qd-1}u_r + u_{qd}u_{r-1}$$

此式中，∵ $u_d | u_k$，$u_d | u_{qd}$（（一）中已证明），所以，$u_d | u_{qd-1}u_r$，但因 u_{qd} 与 u_{qd-1} 互素（相邻两个斐波那契数互素是不难证明的），所以 $u_d | u_r$，但因 $0<r<d$ 且注意 $d \neq 2$（即 $u_d \neq 1$），这是不可能的，由导出的矛盾使该命题得证。

（三）令 $F(x)$ 表示第 x 个斐波那契数，我们证明下面的引理：

对 $x>0$ 且 $0<u\leqslant z$，令

$$\Phi(u,x,z)=(z-u)\cdot F(xu-1)\cdot F(x)$$
$$+F(xu)\cdot F(x-1)$$

那么 $F(x) | z$ 当且仅当 $(F(x))^2 | \Phi(u,x,z)$

证 对 u 施归纳法。首先当 $u=1$ 时，我们有：

$$\Phi(1,x,z)=zF(x-1)\cdot F(x)$$

由 $F(x)$ 和 $F(x-1)$ 是互素的，得出命题成立。若 $u=v$ 时成立，我们看 $u=v+1$ 时。为此，我们希望借助于 $\Phi(v,x,z)$ 来表示 $\Phi(u,x,z)$，为此目的，我们用加法定理容易得到：

$$F(xu-1)=F(xv-1+x)$$
$$=F(xv)F(x)+F(xv-1)$$
$$F(x-1)$$

$$F(xu)=F(xv+x)$$

$$= F(xv+1)F(x)+F(xv)F(x-1)$$

$$F(xv+1)=F(xv)+F(xv-1)$$

使用这些恒等式，由 $\Phi(u,x,z)$的定义，不难得出 $\Phi(u,x,z)$ 与 $\Phi(v,x,z)$ 的关系式：

$$\Phi(u,x,z)=\Phi(v,x,z)F(x-1)+M\cdot F(x)F(xv)$$

这里 $M=(z-u)F(x)+F(x-1)$，由此，并注意到相邻两个斐波那契数是互素的以及本节的（一），我们得到：

$$(F(x))^2\mid\Phi(u,x,z) \quad 当且仅当 \quad (F(x))^2\mid\Phi(v,x,z)$$

由归纳假设命题得证。

（四）引理　对所有的x 和y，若 $(F(x))^2\mid F(y)$则 $F(x)\mid y$。

证　我们假设 $y>x>2$，否则那些情况都是不证自明的。

假若 $(F(x))^2\mid F(y)$，则 $F(x)\mid F(y)$，由（二）我们有$y=xz$，这里 $z>1$。使用（三）中的引理，我们令 $u=z$ 有：

$$F(x)\mid z 当且仅当 (F(x))^2\mid F(xz)\cdot F(x-1)$$

于是 $F(x)\mid z$，所以 $F(x)\mid y$得证。

（五）引理　对所有的x，y，如果$x\cdot F(x)\mid y$，那么$(F(x))^2\mid F(y)$。

证 对 $y=0$是成立的，我们设 $y>0$。

如果 $x\cdot F(x)\mid y$成立，那么 $x>0$ 并且有某个$z>0$ 使 $y=xz$。因此 $F(x)\mid z$，且由（三）中的引理有（令 $u=z$）：

$$(F(x))^2\mid F(y)\cdot F(x-1)$$

但由于$F(x)$与 $F(x-1)$ 是互素的，

$$\therefore\ (F(x))^2\mid F(y) \qquad \square$$

3. 几个重要的引理

（一）我们首先证明关于斐波那契数满足一个刁藩图方程的引理：

方程 $u^2-uv-v^2=1$当且仅当存在着一个 x 使 $u=F(2x+1)$且 $v=F(2x)$。

证 容易用归纳法证明

$$(F(x+1))^2-F(x)F(x+1)-(F(x))^2$$
$$=(-1)^x$$

令 x为偶的，如令 $x=2k$，则有

$u=F(2k+1)$，$v=F(2k)$而使

$u^2-uv-v^2=1$ 成立。

又，若u,v是满足方程

$$(u^2-uv-v^2)^2=1,\ u>0 \qquad (10)$$

那么，对某个 x有：

$$u=F(x+1),\ v=F(x) \qquad (11)$$

我们施归纳于$u+v$。

对 $v=0$时，有 $u=1$，取 $x=0$ 即可，即 $v=F(0)=0$，$u=F(1)=1$（我们用了$F(0)=0$的定义）

现在假定 $v>0$，那么 $u\geqslant v$，否则 u^2-uv-v^2将取负值，我们令 $u'=v$，$v'=u-v$，因此，$u=u'+v'$，$v=u'$，将 u，v代入到（10）式，我们得到

$$(u'^2-u'v'-v'^2)^2=1$$

又，由假设 $u'=v>0$。因为$u'+v'=u<u+v$，我们可以由归纳假设得出，对某个 y，

$$u'=F(y+1),\quad v'=F(y)$$

因此，我们找到

$$u=F(y+1)+F(y)=F(y+2),$$
$$v=F(y+1)$$

因之（11）式对 $x=y+1$也成立。

注意到由 $u^2-uv-v^2=1$ 可推出 $(u^2-uv-v^2)^2=1$ □

（二）令 $\gamma_m(x,y)$ 表示一个自然数上的函数：它取 x 被 y 除的正余数为值（或零）。

引理　令 $d=F(2b)+F(2b+2)$，我们有：

$$\gamma_m(F(2x),d)=F(2x)\text{若}b>0\text{ 且 }x\leqslant b+1 \qquad (12)$$

$$\gamma_m(F(2x),d)=d-F(4b-2x+2)\text{若}$$

$$b\leqslant x\leqslant 2b \tag{13}$$

$$\gamma_m(F(2(x+2b+1)),d)=\gamma_m(F(2x),d) \tag{14}$$

其中（14）式是说函数 $\gamma_m(F(2x),d)$以$2b+1$为周期。

证 （12）式是显然的，因为这种情况下

$$F(2x)<d$$

为了证明（13），在所述的条件下我们发现，

$$0\leqslant F(b)\leqslant d-F(4b-2x+2)\leqslant d-F(2)<d$$

因此，只要证明下面的同余式就足够了：

$$F(2x)\equiv -F(4b-2x+2)\pmod d \tag{15}$$

（对 $b\leqslant x\leqslant 2b$）。

我们施归纳法于 x。对 $x=b$和$x=b+1$ 从（15）由 d 的定义可直接导出。若 x 等于z 和 $z+1$，（15）式成立，我们看 $x=z+2$时，

$$\because\ F(2z+4)=3F(2z+2)-F(2z)$$

$$\therefore\ F(2z+4)\equiv -3F(4b-2z)+F(4b-2z+2)\pmod d$$

$$又\ \because\ F(4b-2z+2)=3F(4b-2z)-F(4b-2z-2)$$

$$\therefore\ F(2z+4)\equiv -F(4b-2z-2)\pmod d$$

$\therefore$（15）式对 $x=z+2$也成立。从而（15）式对 $b\leqslant x\leqslant 2b$都成立（实际上对 $b\leqslant x\leqslant 2b+1$也成立）。 □

此外，我们还指出，（15）式对 $x<b$ 也是成立的，因为在这种情况下，我们令 $u=2b-x+1$，于是 $b+1<u\leqslant 2b+1$，（15）式中用 u 代替 x 已证明是成立的，而将 $u=2b-x+1$ 代入到

$$F(2u)\equiv -F(4b-2u+2)\pmod{d}$$

有

$$F(4b-2x+2)\equiv -F(2x)\pmod{d}$$

这同样是（15）式。

为了证明（14），我们只需证（14′）：

$$F(2x+4b+2)\equiv F(2x)\pmod{d}\qquad(14')$$

我们施归纳于 x，当 $x=0$ 时，我们应指出

$$F(4b+2)\equiv 0$$

这只需在（15）式中令 $x=0$ 即可。

对 $x=1$，我们必须指出 $F(4b+4)\equiv 1$。在（15）式中，置 $x=2b$，我们得到 $F(4b)\equiv -1$，但是由于：

$$F(4b+4)=3F(4b+2)-F(4b)\equiv 0-(-1)$$
$$\equiv 1$$

对归纳步我们置 $x=z+2$ 并再次使用连续偶角标斐波那契数的递推关系而得证。

（三）我们先定义一个二元辅助函数 g，

$$\begin{cases} g(w,0)=0 \\ g(w,1)=1 \\ g(w,x+2)=wg(w,x+1)-g(w,x) \end{cases}\qquad(16)$$

我们只对 $w \geqslant 2$ 的 $g(w,x)$ 感兴趣，对于这样的 w，容易证明（归纳于 x），$g(w,x+1) > g(w,x)$。

使用（16），用归纳于 x 容易看出

$$g(w,x) \equiv x \pmod{w-2}，对 w \geqslant 2 \quad (17)$$

还用归纳于 x 容易看出：

$$F(2x) \equiv g(w,x) \pmod{w-3}，对 w \geqslant 2 \quad (18)$$

下面的引理类似于本节的（一）。

引理 令 $w \geqslant 2$，那么下面两个条件是等价的：

$$u^2 - wuv + v^2 = 1，u \leqslant v \quad (19)$$

对于某个 x，

$$u = g(w,x) 且 v = g(w,x+1) \quad (20)$$

证 (20)$\Longrightarrow$(19)是容易的，使用（16）及施归纳于 x 即可。

为证明(19)$\Longrightarrow$(20)，我们施归纳于 $wv-u$，这由 $u \leqslant v$ 看出，它是正的。

对 $u=0$，由(19) 导出 $v=1$，所以 $x=0$ 时，（20）式成立。

现在令（19）式对 $u>0$ 成立，重新安排（19）我们有：

$$u^2 = 1 + v(wu-v)，0 < u \leqslant v$$

由此我们得到 $0 \leqslant wu - v < u$。令 $u' = wu - v$，

$v'=u$，那么 $u=v'$，$v=wv'-u'$，把 u,v代入到（19），我们有：

$$u'^2-wu'v'+v'^2=1$$

又，我们已看到，$u'=wu-v<u=v'$。由于

$$wv'-u'=v<(w-1)v\leqslant wv-u$$

我们可以用我们的归纳假设得到有某个 y，

$$u'=g(w,y) \text{且} v'=g(w,y+1)$$

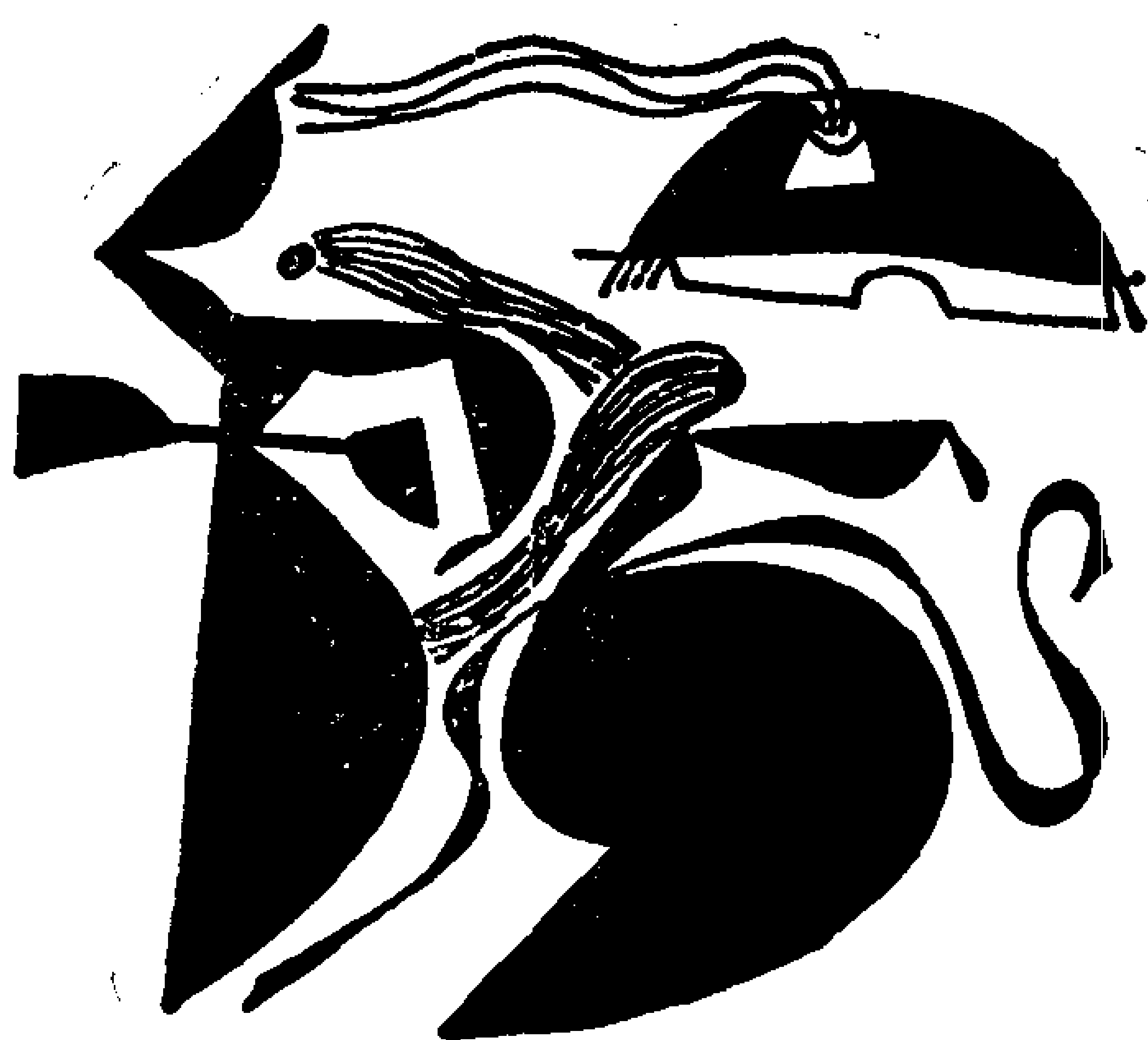
因此，$u=g(w,\ y+1)$且使用（16）有

$$v=g(w,y+2)$$

因此（20）对 $x=y+1$也成立。

本章的关于斐波那契数的性质，多数在后面的章节要用到，这是我们不惜花费一定的篇幅来描述这些的目的所在。

五　贝尔方程



1. 阿基米德分牛问题

我们已经提到，关于刁藩图方程的研究是很古老的，可是那些年代多是一些具体的数学问题，而往往又有一些故事情节和趣味性。

贝尔方程是一类特殊的刁藩图方程，在没有正式描述这类方程前，我们看看一个古老的数学趣题，它是公元前三世纪的希腊数学家阿基米德提出的，称为阿基米德分牛问题：

太阳神有一群牛，由白、黑、花、棕四种颜色的公、母牛组成。在公牛中，白牛数多于棕牛数，多出之数相当于黑牛的$\left(\frac{1}{2}+\frac{1}{3}\right)$；黑牛数多于棕牛数，多出之数相当于花牛数的$\left(\frac{1}{4}+\frac{1}{5}\right)$；花牛数多于棕牛数，多出之数相当于白牛数的$\left(\frac{1}{6}+\frac{1}{7}\right)$。

在母牛中，白牛数是全体黑牛数的$\left(\frac{1}{3}+\frac{1}{4}\right)$；黑牛数是全体花牛数的$\left(\frac{1}{4}+\frac{1}{5}\right)$；花牛数是全体

棕牛数的$\left(\frac{1}{5}+\frac{1}{6}\right)$；棕牛数是全体白牛数的$\left(\frac{1}{6}+\frac{1}{7}\right)$。

问这牛群是怎样组成的？

这个题目看来并不很难，人们把它称作阿基米德问题是考虑到他的辉煌成就，以及他把这个分牛问题献给古希腊后期的著名学者埃拉托斯散这一事实。

这一分牛问题的更完整的形式被莱辛于1773年发现，这是一个希腊文手抄本，该题由22组对偶句组成：

"朋友，请准确无误地数一数太阳神的牛群。要数得十分仔细，如果你自认为还有几分聪明，多少头牛在西西里岛草地上吃过草，它们分为四群，在那里来往踱步。……当所有黑白公牛齐集在一起，就排出一个阵形，纵横相等；辽阔的西西里原野，布满大量的公牛。当棕色公牛与花公牛在一起，便排成一个三角形，一头公牛站在三角形顶端；棕色公牛无一头掉队，花公牛也头头在场，这里没有一头牛和它们的毛色不同.……"

加上了这几行关于公牛的美丽画面，问题变得难多了，这是阿基米德分牛问题的完整题意。

让我们分析一下这个问题，它可有8个未知数来刻画四种颜色及公牛、母牛，由题意可列出

7个方程，又有某些公牛排成方阵，另一些公牛排成三角形又得到必须满足的附加条件，如令 X, Y, Z, T 分别表示白、黑、花、棕各色的公牛数，则附加条件表示为：

$$X+Y=M^2 \quad (1)$$

$$Z+T=\frac{K(K+1)}{2} \quad (2)$$

（1）表示 $X+Y$ 是一个完全平方数，而（2）则表示 $Z+T$ 是一个三角数。

这个牛问题可化为一个二次刁藩图方程：

$$x^2-4729494y^2=1 \quad (3)$$

这个方程的最小解 x 是45位数，y 是41位数，而对应于 x, y 这些值的牛问题的最小解的数字也是异常大的，都是多少万亿只牛，而题中描述的西西里岛上牛的活动场面简直是不可能的！因为这个小岛的面积不过25500平方公里。人们怀疑此题是否出自阿基米德。

方程（3）叫做贝尔方程，它的一般形式是

$$x^2-Ny^2=1$$

这里 N 是非完全平方数。（否则，方程是没什么意思的）

贝尔（1611—1685），是一个伟大的学者和教师，十几岁就进入剑桥的一个学院学习，曾任数学教授，1663年他当选为皇家学会会员。

贝尔本人并未对贝尔方程做过深入的研究，而费马和拉格朗日倒做出了不小贡献。

2. 贝尔方程

贝尔方程的提出和讨论已有几百年甚至更远的历史，然而，当冲击希尔伯特第十问题时，人们却拿起了这个武器，鲁宾逊在1952年首先深入地研究了贝尔方程，它的丰富的性质使得鲁宾逊几乎证明了幂函数可以表示成若干个刁藩图方程组。

贝尔方程的解有着很丰富的性质，有些甚至和斐波那契数的性质很相似，鲁宾逊利用这一武器得到许多成果，成为突破希尔伯特第十问题的第一大进展。

下面我们将详细的研究贝尔方程解的性质，进行较细的推演，我们从下面的贝尔方程（1）入手。

$$\begin{cases} x^2 - dy^2 = 1, & x, y \geqslant 0 \\ d = a^2 - 1, & a > 1 \end{cases} \tag{1}$$

注意到，方程（1）有显然的整数解

$$x = 1 \qquad y = 0$$

$$x = a \qquad y = 1$$

下面我们给出一些有用的引理，它们都是刻

画（1）的整数解的性质。

引理1 不存在整数（正的，负的或零）x, y，它满足方程（1），且

$$1<x+y\sqrt{d}<a+\sqrt{d}$$

证 若 $1<x+y\sqrt{d}<a+\sqrt{d}$

则由 $1=(a+\sqrt{d})(a-\sqrt{d})$

$$=(x+y\sqrt{d})(x-y\sqrt{d})$$

$$\therefore\ x+y\sqrt{d}=\frac{1}{x-y\sqrt{d}}$$

$$a+\sqrt{d}=\frac{1}{a-\sqrt{d}}$$

$$\therefore\ 1<\frac{1}{x-y\sqrt{d}}<\frac{1}{a-\sqrt{d}}$$

$$\therefore\ x-y\sqrt{d}<1$$

$$-x+y\sqrt{d}>-1$$

又 $a-\sqrt{d}<x-y\sqrt{d}$

$$-a+\sqrt{d}>-x+y\sqrt{d}$$

$$\therefore\ -1<-x+y\sqrt{d}<-a+\sqrt{d}$$

$$\therefore\ 0<2y\sqrt{d}<2\sqrt{d}$$

$$\therefore\ 0<y<1$$

这与假设y为整数相矛盾。 □

引理2 若 x, y 及 x', y' 是（1）的整数解，则令

$$x''+y''\sqrt{d}=(x+y\sqrt{d})(x'+y'\sqrt{d})$$

那么，x'',y'' 也是（1）的一组整数解。

证 由$x''+y''\sqrt{d}=(x+y\sqrt{d})(x'+y'\sqrt{d})$

容易得出：$x''-y''\sqrt{d}=(x-y\sqrt{d})(x'-y'\sqrt{d})$

两式相乘有：

$$(x'')^2-d(y'')^2=(x^2-dy^2)((x')^2-d(y')^2)$$
$$=1$$

所以，x'',y'' 也是（1）的整数解。

定义 对于 $n\geqslant 0$，$a>1$，$x_n(a)$，$y_n(a)$由下式定义：

$$x_n(a)+y_n(a)\sqrt{d}=(a+\sqrt{d})^n$$

在以后的叙述中，在不致混淆的情况下，常常用 x_n,y_n 代替 $x_n(a),y_n(a)$。

引理3 x_n,y_n 是（1）的解。

证 应用引理2并用归纳法立刻得证。

引理4 若x,y是（1）的一个非负解，那么，一定存在着某个 n,有：

$$x=x_n,\quad y=y_n$$

证 由于$x+y\sqrt{d}\geqslant 1$，又因为序列$(a+\sqrt{d})$是无限增长的，因而，对某一个$n\geqslant 0$有：

$$(a+\sqrt{d})^n\leqslant x+y\sqrt{d}<(a+\sqrt{d})^{n+1}$$

如若命题不成立，即等式不能成立，于是有：

$$x_n+y_n\sqrt{d}<x+y\sqrt{d}<(x_n+y_n\sqrt{d})(a+\sqrt{d})$$

用 $x_n+y_n\sqrt{d}$ 除，有

$$1<\frac{x+y\sqrt{d}}{x_n+y_n\sqrt{d}}<a+\sqrt{d}$$

注意到 $(x_n+y_n\sqrt{d})(x_n-y_n\sqrt{d})=1$，上式变为：

$$1<(x+y\sqrt{d})(x_n-y_n\sqrt{d})<a+\sqrt{d}$$

$$\therefore\ 1<(xx_n-yy_nd)+(x_ny-xy_n)\sqrt{d}<a+\sqrt{d}$$

令 $x'=xx_n-yy_nd$，$y'=x_ny-xy_n$

则可以验证 x',y' 是方程（1）的一个解：

$$\begin{aligned}&(xx_n-yy_nd)^2-d(x_ny-xy_n)^2\\&=x^2x_n^2-2xyx_ny_nd+y^2y_n^2d^2-d(x_n^2y^2\\&\quad-2xyx_ny_n+x^2y_n^2)\\&=x^2x_n^2+y^2y_n^2d^2-dx_n^2y-dx^2y_n^2\\&=x_n^2(x^2-dy^2)-y_n^2d(x^2-dy^2)\\&=x_n^2-y_n^2d=1\end{aligned}$$

于是有：

$$1<x'+y'\sqrt{d}<a+\sqrt{d}$$

其中 x'，y' 是（1）的一个解，这与引理 1 矛盾。 □

引理 5 （加法定理）

$$x_{m+n}=x_mx_n+dy_my_n$$

$$y_{m+n}=x_ny_m+x_my_n$$

证

$$x_{m+n}+y_{m+n}\sqrt{d}=(a+\sqrt{d})^{m+n}$$
$$=(a+\sqrt{d})^{m}\cdot(a+\sqrt{d})^{n}$$
$$=(x_m+y_m\sqrt{d})(x_n+y_n\sqrt{d})$$
$$=(x_mx_n+dy_my_n)$$
$$+(x_ny_m+x_my_n)\sqrt{d}$$

因此，

$$x_{m+n}=x_mx_n+dy_my_n$$
$$y_{m+n}=x_ny_m+x_my_n$$

类似地，可有：

$$x_{m-n}=x_mx_n-dy_my_n$$
$$y_{m-n}=x_ny_m-x_my_n$$

这可由：

$$(x_{m-n}+y_{m-n}\sqrt{d})(x_n+y_n\sqrt{d})$$
$$=x_m+y_m\sqrt{d}$$
$$\therefore\quad x_{m-n}+y_{m-n}\sqrt{d}=(x_m+y_m\sqrt{d})$$
$$(x_n-y_n\sqrt{d})$$
$$x_{m-n}+y_{m-n}\sqrt{d}=(x_mx_n-dy_my_n)$$
$$+(x_ny_m-x_my_n)\sqrt{d}$$

于是可立即导出。

引理 6　$y_{m\pm1}=ay_m\pm x_m$

$$x_{m\pm1}=ax_m\pm dy_m$$

证　由引理 5，令 $n=1$有：

$$y_{m\pm1}=x_1y_m\pm x_my_1$$

注意到 $x_1=a$，$y_1=1$有

$$y_{m\pm1}=ay_m\pm x_m$$

对第二个式子可类似地证明。

令 (x,y)表示 x,y 的最大公约数，我们有：

引理7 $(x_n,y_n)=1$，即方程（1）的解的两个分量是互素的。

证 若 $d|x_n$（符号"｜"表示整除）且 $d|y_n$ 那么 $d|x_n^2-dy_n^2$，由于 $x_n^2-dy_n^2=1$，

$\therefore d|1$，即 $d=1$ □

引理8 $y_n|y_{nk}$

证 施归纳法于 k，$k=1$ 时，命题显然成立，若$k=m$已成立，应用加法定理（引理5）：

$$y_{n(m+1)}=x_ny_{nm}+x_{mn}y_n$$

由归纳假设，$y_n|y_{nm}$，于是 $y_n|y_{n(m+1)}$，所以对$k=m+1$命题也成立。 □

引理9 $y_n|y_t$ 当且仅当 $n|t$。

证 当 $n|t$时，由引理8有 $y_n|y_t$，所以我们只需证明，如果$y_n|y_t$，则 $n|t$。如若不然，假定 $y_n|y_t$ 但 $n\nmid t$，于是可把 t 表示为：

$$t=nq+r,\ 0<r<n$$

于是有 $y_t=x_ry_{nq}+x_{nq}y_r$

又由于 $y_n|y_{nq}$，所以 $y_n|x_{nq}y_r$，但是 $(y_n,x_{nq})=1$。（因为若$d|y_n$，$d|x_{nq}$，那么由引理8，$d|y_{nq}$，又由引理7，导出 $d=1$。）因此 $y_n|y_r$，但因为

$r<n$，我们有 $y_r<y_n$ （这一点可由引理 6 容易看出），矛盾。

引理10

$$y_{nk}\equiv kx_n^{k-1}y_n(\bmod(y_n)^3)$$

证 $x_{nk}+y_{nk}\sqrt{d}=(a+\sqrt{d})^{nk}$

$$=(x_n+y_n\sqrt{d})^k$$

$$=\sum_{j=0}^{k}\binom{k}{j}x_n^{k-j}y_n^jd^{j/2}$$

$$\therefore\quad y_{nk}=\sum_{\substack{j=1\\ j\text{为奇}}}^{k}\binom{k}{j}x_n^{k-j}y_n^jd^{(j-1)/2}$$

注意到，在这一展开式中，除了 $j=1$，对 $j\geqslant3$的奇数，各分项均含有不低于 $(y_n)^3$，而 $j=1$时，y_{nk} 展开式的第一项为：

$$kx_n^{k-1}y_n$$

$$\therefore\ y_{nk}\equiv kx_n^{k-1}y_n\ (\bmod\ (y_n)^3)$$

引理11 $y_n^2\,|\,y_{ny_n}$

证 由引理10，令 $k=y_n$有：

$$y_{ny_n}\equiv y_n^2x_n^{k-1}\ (\bmod(y_n)^3)$$

$$\therefore\ y_n^2\,|\,y_{ny_n}$$

引理12 若 $y_n^2\,|\,y_t$，那么$y_n\,|\,t$。

证 $\because\ y_n^2\,|\,y_t$，

$\therefore\ y_n\,|\,y_t$，由引理 9

$\therefore\ n|t$

令 $t=nk$,

$\because\ y_n^2|y_{nk}$

由引理10,

$$y_{nk}\equiv kx_n^{k-1}y_n(\bmod (y_n)^3)$$

有 $y_n^2|kx_n^{k-1}y_n$

即 $y_n|kx_n^{k-1}$

由引理7， $(y_n,x_n)=1$

$\therefore\ y_n|k$,因而 $y_n|t$. □

引理13 $x_{n+1}=2ax_n-x_{n-1}$

$y_{n+1}=2ay_n-y_{n-1}$

证 由引理6有:

$$x_{n+1}=ax_n+dy_n$$

$$x_{n-1}=ax_n-dy_n$$

$$\therefore\ x_{n+1}+x_{n-1}=2ax_n$$

即 $x_{n+1}=2ax_n-x_{n-1}$

同理, $y_{n+1}=ay_n+x_n$

$$y_{n-1}=ay_n-x_n$$

$$\therefore\ y_{n+1}+y_{n-1}=2ay_n$$

$$y_{n+1}=2ay_n-y_{n-1}$$

对于方程（1）的解，我们已经知道最初的两个解，让我们分别记为:

$$x_0=1,\ y_0=0$$

$$x_1=a,\ y_1=1$$

在以下的关于方程解的性质的讨论中，我们往往用归纳法证明，要用到上面的事实。

引理14 $y_n \equiv n \pmod{a-1}$

证 对 $n=0,1$ 时，同余式保持，若对 $n=k-1, k$ 时同余式保持，则

$$\begin{aligned} y_{k+1} &= 2ay_k - y_{k-1} \\ &\equiv 2y_k - y_{k-1} \text{（使用}a\equiv 1 \pmod{a-1}\text{）} \\ &\equiv 2k-(k-1) \text{（使用归纳假设）} \\ &\equiv k+1 \pmod{a-1} \end{aligned}$$

从而同余式对 $n=k+1$时也成立。 □

引理15 若 $a\equiv b \pmod c$，那么，对所有的n，

$$x_n(a)\equiv x_n(b) \pmod c$$

$$y_n(a)\equiv y_n(b) \pmod c$$

证 $n=0,1$ 时，同余式成立，这是容易验证的。

$$\because\ 1\equiv 1 \pmod c$$

$$\therefore\ x_0(a)\equiv x_0(b) \pmod c$$

$$\because\ a\equiv b \pmod c$$

$$x_1(a)\equiv x_1(b) \pmod c$$

且由于$y_0=0$，$y_1=1$均为常数，对 y_n的同余式更是明显的。

若 $n=k-1, k$ 同余式成立，则

$$y_{k+1}(a)=2ay_k(a)-y_{k-1}(a)$$

$$\equiv 2by_k(b) - y_{k-1}(b) \pmod{c}$$

$$= y_{k+1}(b)$$

所以，对 $n=k+1$时同余式也成立。对 x_n 的同余式的证明，方法完全相同。

引理16 n 和 y_n 同奇偶。

证 由引理13有：

$$y_{n+1} = 2ay_n - y_{n-1}$$

$$\therefore\ y_{n+1} \equiv y_{n-1} \pmod{2}$$

∴ 当n为偶的有

$$y_n \equiv y_0 = 0 \pmod{2}$$

当 n为奇的有

$$y_n \equiv y_1 = 1 \pmod{2}$$

引理17

$$x_n(a) - y_n(a)(a-y) \equiv y^n \pmod{2ay - y^2 - 1}$$

证 由于 $x_0 - y_0(a-y) = 1$,

$$x_1 - y_1(a-y) = y$$

所以对 $n=0,1$时命题成立。

假设对 $n=k-1,k$时命题成立，对$n=k+1$时，

$$x_{k+1} - y_{k+1}(a-y) = 2a[x_k - y_k(a-y)] - [x_{k-1} - y_{k-1}(a-y)]$$

$$\equiv 2ay^k - y^{k-1} \pmod{2ay - y^2 - 1}$$

$$= y^{k-1}(2ay-1)$$

注意到 $2ay-1 \equiv y^2 \pmod{2ay-1-y^2}$

代入上式有：

$$x_{k+1}-y_{k+1}(a-y)\equiv y^{k-1}\cdot y^2$$
$$\equiv y^{k+1}\pmod{2ay-y^2-1}$$

即对于 $n=k+1$时命题也成立。 □

引理18　对所有的 n，$y_{n+1}>y_n\geqslant n$。

证　由引理 6 并注意到 $y_0=0\geqslant 0$，立刻得证。 □

引理19　对所有的 n，

$$x_{n+1}(a)>x_n(a)\geqslant a^n$$
$$x_n(a)\leqslant(2a)^n$$

证　由引理 6 和13

$$ax_n(a)\leqslant x_{n+1}(a)\leqslant(2a)x_n(a)$$

用归纳法立刻可得出结果。

下面是序列 x_k中的某些周期性质。

引理20　$x_{2n\pm j}\equiv -x_j\pmod{x_n}$

证　由引理 5 有：

$$x_{2n\pm j}=x_nx_{n\pm j}+dy_ny_{n\pm j}$$
$$\equiv dy_n(y_nx_j\pm x_nx_j)\pmod{x_n}$$
$$\equiv dy_n^2x_j\pmod{x_n}.$$
$$=(x_n^2-1)x_j$$
$$\equiv -x_j\pmod{x_n}$$
□

引理21　$x_{4n\pm j}\equiv x_j\pmod{x_n}$

证　由引理20有：$(4n\pm j=2n+(2n\pm j))$

$$x_{4n\pm j}\equiv -x_{2n\pm j}\equiv x_j\pmod{x_n}$$

引理22

若 $x_i \equiv x_j \pmod{x_n}$，$i \leqslant j \leqslant 2n$，$n > 0$

那么 $i = j$ 除非 $a = 2$，$n = 1$，$i = 0$ 及 $j = 2$

证 首先假定 x_n 是奇的且令

$$q = (x_n - 1)/2$$

那么数

$$-q, -q+1, -q+2, \cdots, -1, 0, 1, \cdots, q-1, q$$

是模 x_n 的互不同余的完全剩余系。由引理19有，

$$1 = x_0 < x_1 < \cdots < x_{n-1}$$

应用引理 6，$x_{n-1} \leqslant x_n/a \leqslant \frac{1}{2} x_n$；所以 $x_{n-1} \leqslant q$。

又由引理20，数

$$x_{n+1}, x_{n+2}, \cdots, x_{2n-1}, x_{2n}$$

对模 x_n 相应的同余于

$$-x_{n-1}, -x_{n-2}, \cdots, -x_1, -x_0 = -1$$

因此，数 $x_0, x_1, x_2, \cdots, x_{2n}$ 对模 x_n 是彼此不同余的。这就给出了所需的结果。

下面，假设 x_n 是偶的并令 $q = x_n/2$，在这种情况下，数

$$-q+1, -q+2, \cdots, -1, 0, 1, \cdots, q-1, q$$

是对模 x_n 互不同余的完全剩余系。（$\because$ $-q \equiv q \bmod x_n$），同上所述有 $x_{n-1} \leqslant q$，因此结果也如同上述得出，只是有一例外情况：

$$x_{n-1} = q = x_n/2，使得\ x_{n+1} \equiv -q \pmod{x_n}，$$

在这一情况下，$i=n-1$，$j=n+1$ 与我们的结果相矛盾。但由引理 6 有，

$$x_n=ax_{n-1}+dy_{n-1}$$

所以，由 $x_n=2x_{n-1}$可导出$a=2$，$y_{n-1}=0$，即 $n=1$。所以结果仅对 $a=2$，$n=1$，$i=0$，$j=2$ 失效。 □

引理23

若 $x_j\equiv x_i \pmod{x_n}$，$n>0$，$0<i\leqslant n$，$0\leqslant j<4n$。那么，或 $j=i$ 或 $j=4n-i$。

证　首先假设 $j\leqslant 2n$，那么由引理22有 $j=i$（除非特殊情况出现），因为 $i>0$，所以这特殊情况只当 $j=0$才发生，但此时

$$i=2>1=n，这与\ i\leqslant n矛盾。$$

另一方面，若 $j>2n$，令$\bar{J}=4n-j$使

$$0<\bar{J}<2n$$

由引理21有$x_{\bar{J}}\equiv x_j\equiv x_i \pmod{x_n}$

再次应用引理22，并注意此时 $i,\bar{J}>0$，引理22之意外情况不会发生，所以有

$$\bar{J}=i$$

于是 $i=4n-j$，$j=4n-i$ □

引理24　若 $0<i\leqslant n$且 $x_j\equiv x_i \pmod{x_n}$ 那么，$j\equiv \pm i \pmod{4n}$

证　记 $j=4nq+\bar{J}$，$(0\leqslant\bar{J}<4n)$

由引理21，

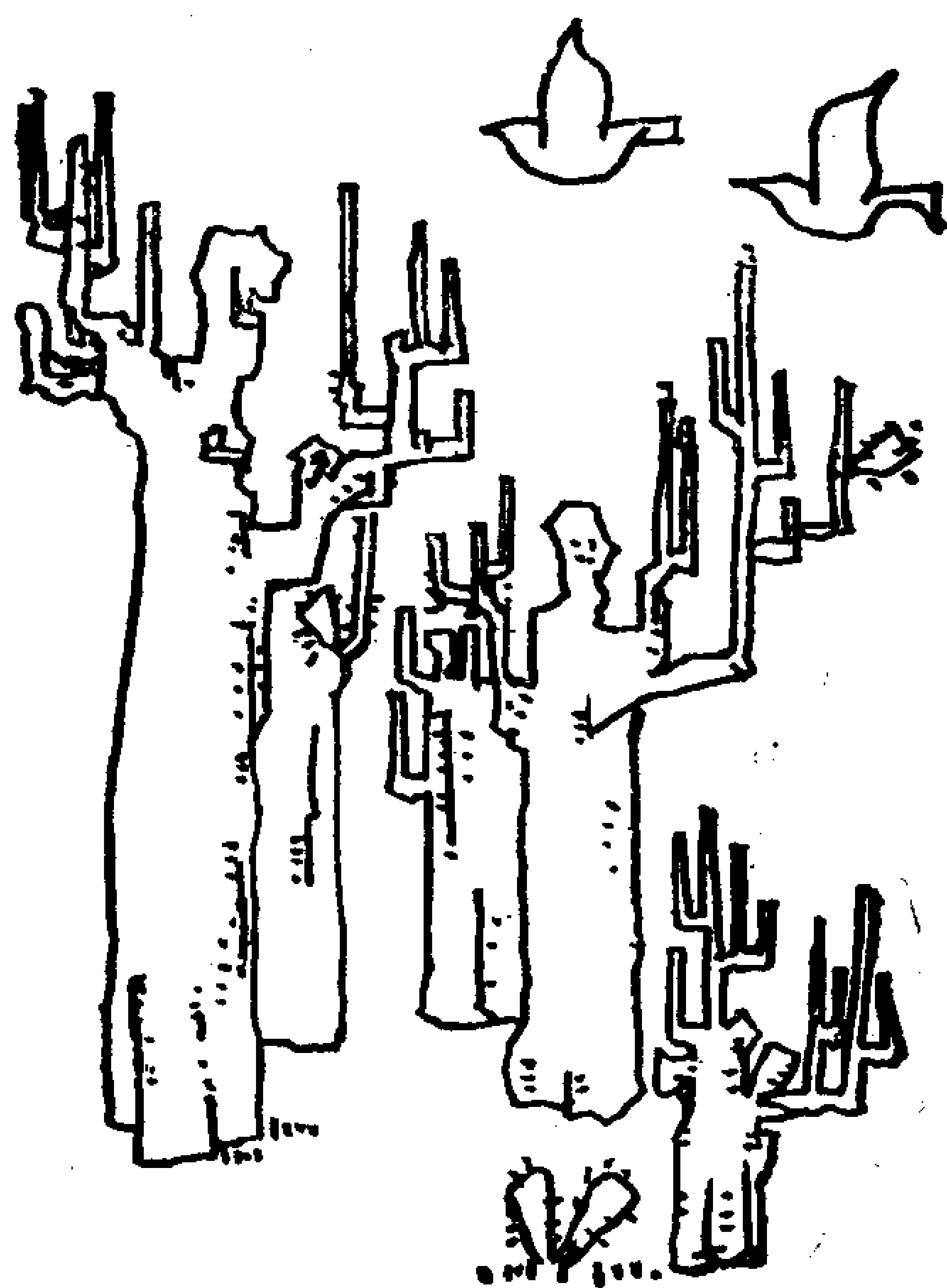
$$x_i \equiv x_j \equiv x_{\overline{J}} \pmod{x_n}$$

由引理23

$$i = \overline{J} \text{或} i = 4n - \overline{J}$$

所以 $j \equiv \overline{J} \equiv \pm i \pmod{4n}$

六 刁藩图集与刁藩图函数



1. 刁藩图集

在引进刁藩图集这一概念之前，我们先直观的看某些自然数集合N的子集。

（1）偶数的集合E：

$E=\{0,2,4,\cdots\}$

（2）奇数的集合D：

$D=\{1,3,5,7,\cdots\}$

（3）斐波那契数的集合 F：

$F=\{1,2,3,5,8,\cdots\}$

（4）合数的集合C：

$C=\{4,6,8,9,10,\cdots\}$

（5）素数的集合 P：

$P=\{2,3,5,7,\cdots\}$

（6） 2的（正）方幂的集合 T：

$T=\{2,4,8,16,32,\cdots\}$

等等，我们还可以举出更多例子。

让我们分析一下这些集合的性质：

第一它们都是无穷集，由于可以和 N 建立1—1对应，所以都是可数无穷集。

第二是任给一个自然数m，m 是否属于这些中的一个集合是可以知道的，即在有穷步内可判定出这一事实。

第三是这些集合的"复杂"程度不一，即产生这一集合的过程（函数）是有着难易之分的。

如产生奇数的函数可写为

$$f(x)=2x+1,\ D=\{f(0),f(1),f(2),\cdots\}$$

产生斐波那契数的函数

$$F(n)=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}$$

$$F=\{F(1),F(2),F(3),\cdots\}$$

（在集合中，相同的元素合并）

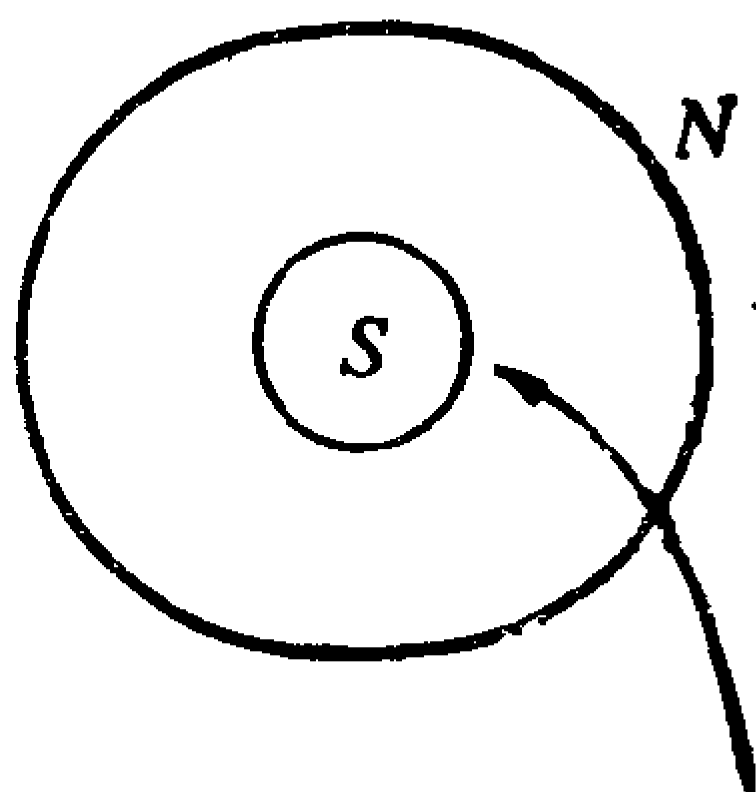
至于用一个函数产生素数，则是相当复杂的，直观的用一"筛子"（即筛法），逐步筛出一个个素数也是在有穷步可以完成的，但可见其复杂程度。

对于（6），它的特点是增长快，从增长速度的观点来看函数的复杂度，自然（6）也不能算简单的，后面我们会看到它的复杂性。

我们通过上述几个例子看到，N 的某些子集是由一个性质或谓词 $P(x)$ 来刻画的，即对子集 $S\subset N$，有

$$S=\{x\,|P(x)\}$$

或 $x \in S \Longleftrightarrow P(x)$ 如下图所示：



S中元有P性质

下面我们来定义刁藩图集，它是和多项式紧密相关的。

定义 1　$P(x_1, x_2, \cdots, x_k)$称为一个多项式，如果$P(x_1, \cdots, x_k)$可表示为函数

$$\sum_{\substack{0 \leq i_1 \leq n_1 \\ 0 \leq i_2 \leq n_2 \\ \cdots \\ 0 \leq i_k \leq n_k}} a_{i_1 i_2 \cdots i_k} x_1^{i_1} x_2^{i_2} \cdots x_k^{i_k}$$

这里 $a_{i_1 i_2 \cdots i_k}$ 是整数（正整数，负整数，零），而变元 $x_1, x_2, \cdots, x_k$ 的变域是 N。

定义 2　一个正整数的有序 n 元组的集合 S 称做刁藩图的，如果存在一个整系数多项式 $P(x_1, \cdots, x_n, y_1, \cdots, y_m)$，这里$m \geq 0$，任给一个$n$元组$\langle x_1, \cdots, x_n \rangle$属于 S当且仅当存在正整数$y_1, \cdots, y_m$ 使

$$P(x_1, \cdots, x_n, y_1, \cdots, y_m) = 0$$

我们用符号“$\Longleftrightarrow$”表示“当且仅当”，借助

于逻辑符号，集合S 和多项式 P 之间的关系可写为：

$$\langle x_1,\cdots,x_n\rangle\in S\Longleftrightarrow(\exists y_1,\cdots,y_m)$$
$$[P(x_1,\cdots,x_n,y_1,\cdots,y_m)=0]$$

或等价的写为：

$$S=\{\langle x_1,\cdots,x_n\rangle\mid(\exists y_1,\cdots,y_m)[P(x_1,\cdots,$$
$$x_n,y_1,\cdots,y_m)=0]\}$$

下面举几个刁藩图集的例子：

(i) 合数的集合：

$$x\in S\Longleftrightarrow(\exists y,z)[x=(y+1)(z+1)]$$

(ii) 非 2 的方幂的集合：

$$x\in S\Longleftrightarrow(\exists y,z)[x=y(2z+1)]$$

(iii) 正整数上的序关系，即集合

$$\{\langle x,y\rangle\mid x<y\},\ \{\langle x,y\rangle\mid x\leqslant y\}$$

$$x<y\Longleftrightarrow(\exists z)(x+z=y)$$

$$x\leqslant y\Longleftrightarrow(\exists z)(x+z-1=y)$$

(iv) 可除性关系，即集合$\{\langle x,y\rangle\mid x|y\}$：

$$x|y\Longleftrightarrow(\exists z)(xz=y)$$

(v)偶角标斐波那契数的集合，即

$$S=\{u_2,u_4,u_6,u_8,\cdots\}$$
$$=\{1,3,8,21,\cdots\}$$

$$x\in S\Longleftrightarrow(\exists y)(5x^2+4=y^2)$$

这一表示式从斐波那契数的性质：（见第四章，3）

u_{2k+1}, u_{2k} $(k=1,2,\cdots)$满足方程

$$u^2-uv-v^2=1$$

即 $u^2-uv-(v^2+1)=0$

其判别式Δ必为一完全平方数，即存在着 m 使 $v^2+4(v^2+1)=m^2$

$$\therefore\ 5v^2+4=m^2$$

从而 (v)的表示成立。

(vi) $\langle x,y,z\rangle$的集合 w，它表示 $x|y$且 $x<z$，表示如下：

$$x|y \Longleftrightarrow (\exists u)(y=xu),$$

$$x<z \Longleftrightarrow (\exists v)(z=x+v)$$

$$\therefore\ \langle x,y,z\rangle \in w \Longleftrightarrow (\exists u,v)[(y-xu)^2+(z-x-v)^2=0]$$

注意到这一技巧是完全一般的，在定义一个刁藩图集时，对多项式的联立方程组

$$P_1=0,\ P_2=0,\cdots,\ P_k=0$$

可以用单一的一个方程来替代：

$$P^2_1+P^2_2+\cdots+P^2_k=0$$

这从逻辑上容易看出：

$$(\exists r_1,\cdots,r_n)[P_1=0]\,\&\,(\exists s_1,\cdots,s_m)[P_2=0]$$
$$\Longleftrightarrow (\exists r_1,\cdots,r_n,s_1,\ \cdots,s_m)[P^2_1+P^2_2=0]$$

对于“或”（$\vee$），也有类似的性质：

$$(\exists r_1,\cdots,r_n)[P_1=0]\vee(\exists s_1,\cdots,s_m)[P_2=0]$$
$$\Longleftrightarrow (\exists r_1,\cdots,r_m,s_1,\cdots,s_m)\ [P_1P_2=0]$$

这就意味着对产生刁藩图集的表达式间使用与(&)和，或(∨)产生出的表达式仍定义一个刁藩图集.

(vii)斐波那契数的集合.

$$x\in S\Longleftrightarrow(\exists u,v)[(u^2-uv-v^2=1)$$
$$\&(x=u\vee x=v)]$$

由于(vi)中我们已说明了“&”,“∨”是可以随意用的，因而这个集合也是刁藩图集.

对于素数集合是刁藩图的这件事证明起来并不容易，表面上它只是“合数”的否定（稍差一个特殊的“1”），实际上，“非”（┐，—)运算对刁藩图集并不是封闭的，一个集合和它的补集既使都是刁藩图的，但证明它们的难度会有天壤之别，2的方幂的集合及其补集都是刁藩图的，但证明前者却异常困难，下一章会看到这一点.同样，证明素数集是刁藩图的还依赖于一个极重要的定理.

2. 刁藩图函数

我们以后把一个函数理解为自变量是正整数，函数值也是正整数.

定义 一个 n元函数 $f(x_1,\cdots,x_n)$称为是刁藩图的，如果

$$\{\langle x_1,\cdots,x_n,y\rangle \mid y=f(x_1,\cdots,x_n)\}$$

是一个刁藩图集. 即，f 是刁藩图的，如果它的图是刁藩图的。

以后我们会回答，什么函数是刁藩图的。

（一）配对函数

在递归函数论中，有一配对函数的技巧是必不可少的，我们会看到，它实质上是建立 $N\times N\to N$上的一一对应，这里我们建立$N^+\times N^+\to N^+$上的一一对应，N^+ 是正整数集。为此，我们列出一个对应三角形：

X \ Y	1	2	3	4	5	6	7	…	…
1	1	3	6	10	·				
2	2	5	9	·					
3	4	8	·						
4	7	·							
5	·								
6									
7									
⋮									

即

$1\longleftrightarrow\langle 1,\ 1\rangle$

$2\longleftrightarrow\langle 2,\ 1\rangle$

$3\longleftrightarrow\langle 1,\ 2\rangle$

$4\longleftrightarrow\langle 3,\ 1\rangle$

$5 \longleftrightarrow \langle 2,\ 2 \rangle$

$6 \longleftrightarrow \langle 1,\ 3 \rangle$

$7 \longleftrightarrow \langle 4,\ 1 \rangle$

$8 \longleftrightarrow \langle 3,\ 2 \rangle$

$9 \longleftrightarrow \langle 2,\ 3 \rangle$

$10 \longleftrightarrow \langle 1,\ 4 \rangle$

· · · · · · ·

我们把上面的对应可记为：

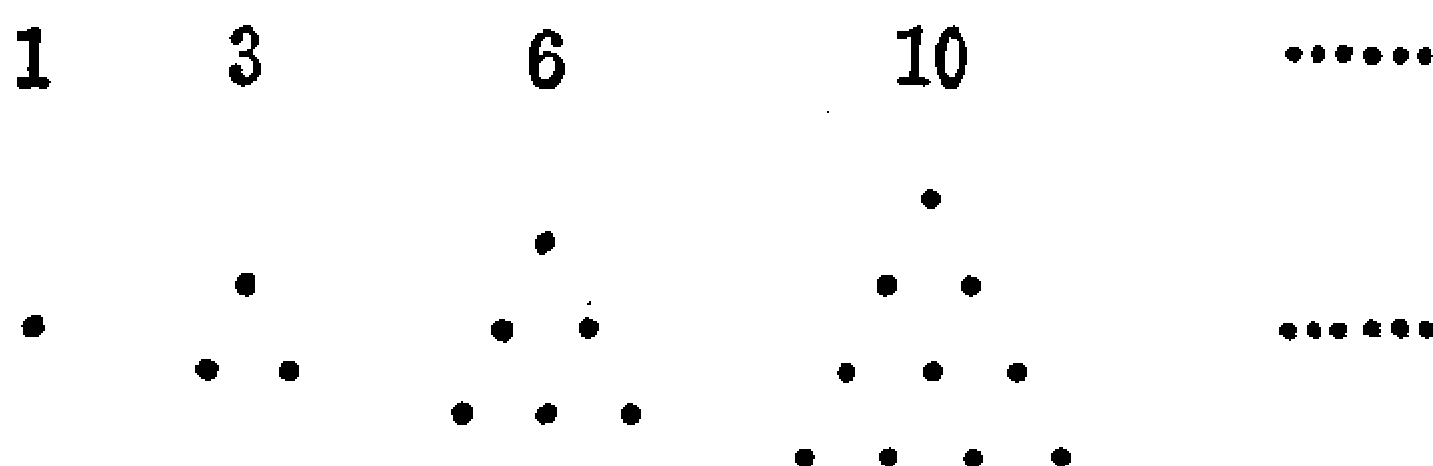
$$z \longleftrightarrow \langle x, y \rangle$$

下面我们找出这一对应关系的表达式。

首先，我们定义三角数 $T(n)$：

$$T(n) = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

$T(n)$ 的名字是由于它可排列成三角形点阵，例如前几个三角数及其点阵如下：



我们看到 $T(n)$ 是递增的，所以，对每个正整数z，总存在着唯一的$n \geqslant 0$

$$T(n) < z \leqslant T(n+1) = T(n) + n + 1$$

于是 z 可唯一的表示为

$$z = T(n) + y;\quad y \leqslant n + 1$$

由 $y\leqslant n+1$有 $y<n+2$，令 $x=(n+2)-y$

于是有 $n=x+y-2$

$\therefore\ z=T(x+y-2)+y$

$$z=\frac{(x+y-1)(x+y-2)}{2}+y$$

令 $P(x,y)=T(x+y-2)+y$

又可由 z唯一地决定 x,y，分别记为

$$x=L(z),\quad y=R(z)$$

容易证明$L(z)$，$R(z)$，$P(x,y)$都是刁藩图函数。因为：

$$z=P(x,y)\Longleftrightarrow 2z=(x+y-2)(x+y-1)+2y$$

$$x=L(z)\Longleftrightarrow(\exists y)[2z=(x+y-2)(x+y-1)+2y]$$

$$y=R(z)\Longleftrightarrow(\exists x)[2z=(x+y-2)(x+y-1)+2y]$$

这里显然还有 $x\leqslant z$，$y\leqslant z$，于是我们可有下面的定理。

定理6.1 （配对函数定理）

存在着这样的刁藩图函数 $P(x,y)$，$L(z)$，$R(z)$，

（1）对所有的 x,y，$L(P(x,y))=x$，$R(P(x,y))=y$ 而且

（2）对所有的z，$P(L(z),R(z))=z$，$L(z)$

$\leqslant z$，$R(z)\leqslant z$。

这一定理最早康托用于证明有理数与整数是一样多的，而为后人精确刻化了。

（二）序列数定理

下面我们利用中国剩余定理及配对函数证明一个很有用的定理。

我们定义一个函数 $S(i,u)$：

$S(i,u)=w$，这里 w是唯一这样的正整数，

$$w\equiv L(u)\ (\bmod\ 1+iR(u))$$

$$w\leqslant 1+iR(u)$$

这里，w是$L(u)$被 $1+iR(u)$除的正余数。

定理6.2 （序列数定理）

存在着一个这样的刁藩图函数 $S(i,u)$，

（1） $S(i,u)\leqslant u$

（2） 对于任一序列 $a_1,a_2,\cdots,a_N$，存在着一个这样的数 u，

$$S(i,u)=a_i,\ 1\leqslant i\leqslant N$$

证 先证明 $S(i,u)$ 是刁藩图的。由上面的定义有：$S(i,u)=w$当且仅当以下方程组有一个解：

$$2u=(x+y-2)(x+y-1)+2y$$

$$x=w+z(1+iy)$$

$$1+iy=w+v-1$$

这是由于 u是 x,y的配对函数，$x=L(u)$，$y=$

$R(u)$，这第二式即：

$$L(u)=w+z(1+iR(u))$$

w是 $L(u)$ 被 $1+iR(u)$ 除的正余数；而第三式即

$$1+iR(u)\geqslant w$$

由我们前面叙述的关于刁藩图方程组的定理，可以看出 $S(i,u)$是刁藩图的。

又，$S(i,u)\leqslant L(u)\leqslant u$。令 $a_1,\cdots,a_N$ 是给定的一个数列，选取某一数 y是大于$a_1,\cdots,a_N$且被 $1,2,\cdots,N$所除尽的，则

$$1+y,\ 1+2y,\cdots,1+Ny$$

是一个互素的数列，这是因为，若 $d|1+iy$ 且 $d|1+jy$，$i<j$，那么 $d|[j(1+iy)-i(1+jy)]$即 $d|j-i$,所以 $d\leqslant N$，这导出 $d|y$，除非$d=1$,否则是不可能的．于是我们可以应用中国剩余定理，得到这样的 x：

$$x\equiv a_1 \pmod{1+y}$$

$$x\equiv a_2 \pmod{1+2y}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

$$x\equiv a_N \pmod{1+Ny}$$

令 $u=P(x,y)$,所以 $x=L(u)$，$y=R(u)$ 且

$$a_i\equiv L(u) \pmod{1+iR(u)}$$

$$(i=1,2,\cdots,N)$$

且 $a_i<y=R(u)<1+iR(u)$,于是依定义，

$$a_i = S(i,u)$$ □

3. 普特南定理

正整数刁藩图集一个重要特性是由普特南于1960年给出了，它使我们对刁藩图集有了深刻而直观的认识。

定理6·3 一个正整数集 S 是刁藩图的当且仅当存在一个多项式 P，S 恰是 P 的正整数值域。

证 若有一个多项式 $P(x_1,\cdots,x_m)$，S恰是P的正整数值域，于是

$$x \in S \Longleftrightarrow (\exists x_1,\cdots,x_m)[x = P(x_1,\cdots,x_m)]$$

所以，S 是一个刁藩图集。

反之，若 S 是一个正整数的刁藩图集，令

$$x \in S \Longleftrightarrow (\exists x_1,\cdots,x_m)$$
$$[Q(x,x_1,\cdots,x_m) = 0]$$

令 $P(x,x_1,\cdots,x_m) = x[1 - Q^2(x,x_1,\cdots,x_m)]$

则P就是我们所求的那个多项式．这是因为，若 $x \in S$，选择 $x_1,\cdots,x_m$ 使

$$Q(x,x_1,\cdots,x_m) = 0$$

那么，$P(x,x_1,\cdots,x_m) = x$，所以，x 是在 P 的值域中．另一方面，若

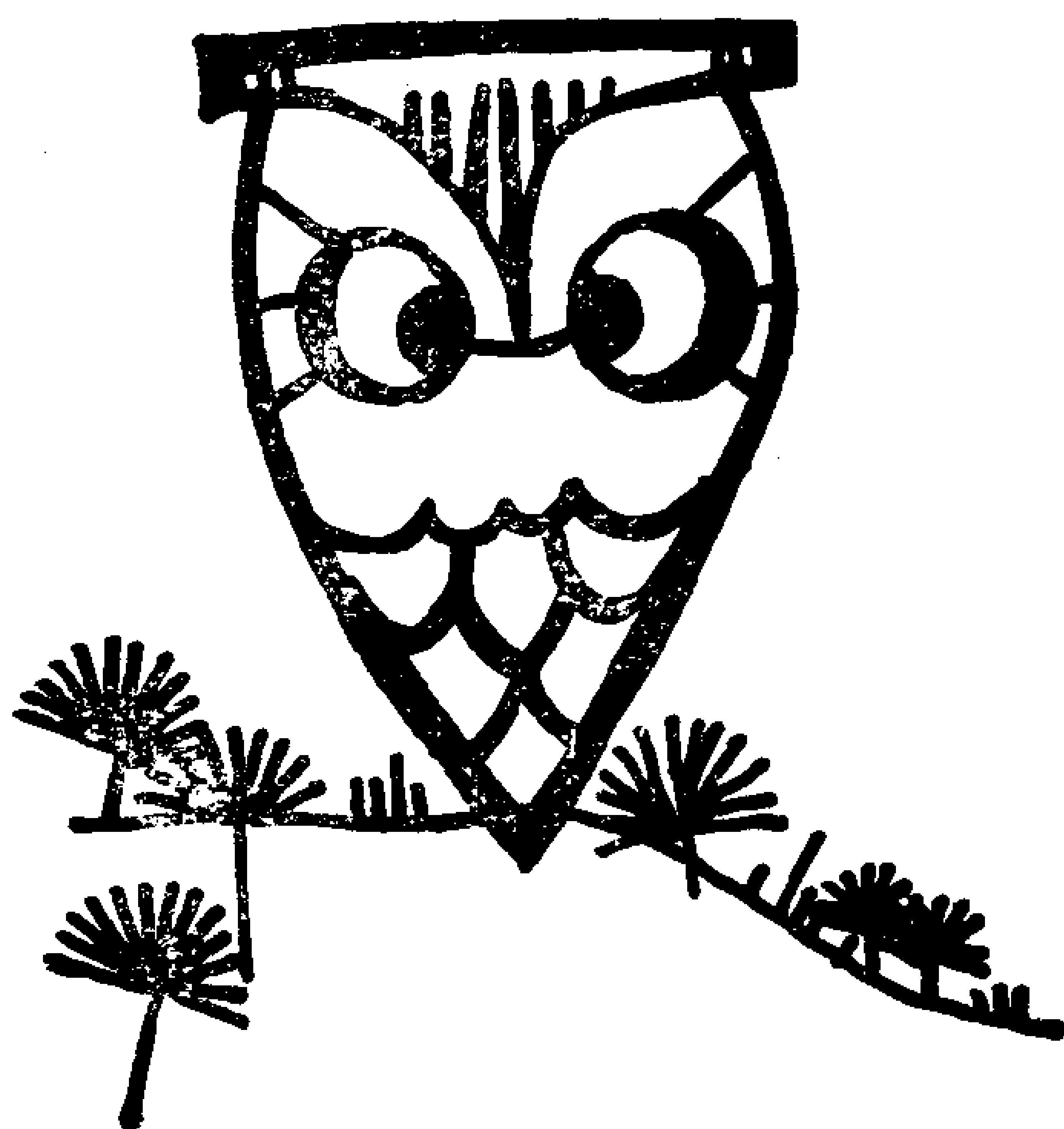
$$z = P(x,x_1,\cdots,x_m), \quad z > 0$$

那么$Q(x,x_1,\cdots,x_m)$必成为零，否则

$$1-Q^2(x,x_1,\cdots,x_m)\leqslant 0$$

因之，$z=x$，于是 $x\in S$。 □

七　幂函数是刁藩图的



一个多项式 $P(x_1,\cdots,x_n,y_1,\cdots,y_m)$，则

$$(\exists y_1,\cdots,y_m)[P(x_1,\cdots,x_n,y_1,\cdots,y_m)=0]$$

称做刁藩图谓词。

如果我们把多项式 P 的整系数中正负分类，则可产生两个具有正整系数的多项式P_1,P_2，使 $P(x_1,\cdots,x_n,y_1,\cdots,y_m)=0$等价于

$$P_1(x_1,\cdots,x_n,y_1,\cdots,y_m)=P_2(x_1,\cdots,x_n,y_1,\cdots,y_m)$$

于是刁藩图谓词还可如下定义：

定义 令 $P(x_1,\cdots,x_n,y_1,\cdots,y_m)$， $Q(x_1,\cdots,x_n,y_1,\cdots,y_m)$ $(m\geqslant 0)$ 是正整系数多项式，则

$$(\exists y_1,\cdots,y_m)[P(x_1,\cdots,x_n,y_1,\cdots,y_m)=Q(x_1,\cdots,x_n,y_1,\cdots,y_m)]$$

叫做刁藩图谓词。

我们看到，上述定义中的多项式只需用自然数，变元，+，×，=，来产生，而刁藩图谓词则再加上一条：可使用存在量词。

自然我们会问，由自然数，+，×，存在量词（变元和“=”是可使用的）会“滚”出多少东

西？这实质上是反映刁藩图谓词（刁藩图集）类有多么大。这涉及到了希尔伯特第十问题的核心。

1952年，沉睡多年的希尔伯特第十问题有了第一次重大进展，美国数学家鲁宾逊在一个假定条件下证明了幂函数是刁藩图的。

鲁宾逊的定理是：〔1〕

谓词$\alpha=\beta^{u}$可用谓词 $x+y=z$，$x\cdot y=z$和任一具有指数级增长的二目谓词 $\rho(x,y)$存在的定义。

这里这一指数级增长的谓词（或关系）$\rho(x,y)$ 的存在称为鲁宾逊假设，它满足下面两个条件，并且是刁藩图的：

（1）$(\forall x,y)(\rho(x,y)\rightarrow y<x^{x})$

（2）$(\forall k)(\exists x,y)(\rho(x,y)\,\&\,y\geqslant x^{k})$

用我们现在的语言解释这个定理是说：用加法、乘法及一个具有指数级增长的二目谓词（或称二元关系），并可使用存在量词可定义出幂函数。

这个定理是鲁宾逊在企图证明幂函数是刁藩图的，由于加、乘已是刁藩图的了，存在量词在定义刁藩图集（谓词）时又可允许使用，从而问题的疑点在于这一指数级增长的二元刁藩图关系是否存在。从而人们在开始寻找满足鲁宾逊假设

的这一谓词。

过了几年，戴维斯、普特南、鲁宾逊于1961年又有了重大突破，他（她）们证明了：

定理〔5〕

任何递归可枚举集都是指数刁藩图的。

这里所谓指数刁藩图的是指可通过下面的方式来定义谓词或函数：

$$(\exists u_1,\cdots,u_n,\ v_1,\cdots,v_n,\ w_1,\cdots,w_n)[P(x_1,\cdots,x_m,u_1,\cdots,u_n,v_1,\cdots,v_n,w_1,\cdots,w_n)=0\ \&\ u_1=v_1^{w_1}\ \&\cdots\&\ u_n=v_n^{w_n}]$$

上面这个结果是十分重要的，实际上，只要把定理中“指数刁藩图的”的中的“指数”二字去掉，希尔伯特第十问题就会迎刃而解：任给一个刁藩图方程，它是否可解是不存在一个算法的。或称希尔伯特第十问题是递归不可解的。

上述定理最初是由戴维斯和普特南得到，基于他们1958年的结果，除利用了他们的结果，还利用了一个迄今未能证明的数论假设：存在着具有任意有限长度的全由素数组成的算术级数。稍后，鲁宾逊参加进来，她发现上述数论假设是不必要的，并大大简化了全部证明。

从上面这个定理我们看出，通向成功之路是解决幂函数是刁藩图的，而这一点又必须找到一个满足鲁宾逊假设的刁藩图谓词。

人们大约寻找了十年，才被苏联数学家马吉雅塞维奇幸运地找到了，他找到的不是别的，正是斐波那契数，我们将证明集合

$$D=\{\langle u,v\rangle \mid v=a_{2u}\&u\geq 2\}$$

（这里 a_{2u} 是第$2u$ 个斐波那契数）

是刁藩图的且满足鲁宾逊假设，从而希氏第十问题这一难题，人们经过七十年的努力，终于于1970年解决了。

1．偶角标斐波那契函数是刁藩图的

我们首先从历史的本来面目，证明最重要的一个定理，它是鲁宾逊假设的一个例证，是添补了由戴维斯、鲁宾逊、普特南建立的宏伟碑石的一个裂缝。

定理7·1 （马吉雅塞维奇）〔6〕

$F(2x)$是第$2x$ 个斐波那契数，则$y=F(2x)$是刁藩图的.

证 我们指出，对任何数 $x,y,F(2x)=y$当且仅当存在着数 r,s,t,u,v,w 使下面 (i)——(viii)成立：

(i) $x\leqslant y<t$

(ii) $t^2-tz-z^2=1$

(iii) $r^2-2rs-4s^2=1$

(iv) $t^2|r$

(v) $w=3+(4s+r)s$

(vi) $u^2-wuv+v^2=1$

(vii) $x=\gamma_m(u,t)$

(viii) $y=\gamma_m(u,4s+r)$

我们将利用第四章的结果证明这个定理。

首先假定，对给的 x, y，存在着数 r, s, t, u, v, z, w 满足条件 (i)——(viii)

由第四章3，（一），从(ii)，对某 a 有

$$t=F(a)$$

从 (iii)，对某 b 有

$$r=F(2b+1)$$

$$2s=F(2b)$$

由 (vi)及第四章3，（三），对某 c 有

$$u=g(w,c)$$

令 $d=F(2b)+F(2b+2)$

于是我们有

$$d=2F(2b)+F(2b+1)=4s+r,$$

由 (viii)我们有

$$y=\gamma_m(g(w,c),d)$$

由第四章（18）式有

$$F(2c)\equiv g(w,c) \pmod{w-3}$$

由 (v)，

$$w=3+(4s+r)s=3+ds$$

所以得到

$$F(2c)\equiv g(w,c) \pmod{ds}$$

$$\therefore\quad F(2c)\equiv g(w,c) \pmod{d}$$

因此有

$$y=\gamma_m(F(2c),d)$$

令 c被 $2b+1$除有商 q和余数 e,即

$$c=q\cdot(2b+1)+e,\quad e\leqslant 2b$$

由第四章3，（二）

$$\because\quad c\equiv e \pmod{2b+1}$$

$$\therefore\quad y=\gamma_m(F(2e),d)$$

我们想知道 e的更精确的范围，即

$e\leqslant b$还是 $b<e\leqslant 2b$

若 $b<e\leqslant 2b$,由第四章3，（二）有

$$y=d-F(4b-2e+1)\geqslant d-F(2b)$$

$$=F(2b+2)$$

但由 (i)和 (iv)有

$$y<t\leqslant r=F(2b+1)\leqslant F(2b+2)$$

这是不可能的，所以有 $e\leqslant b$。

若 $b=0$,则 $d=F(0)+F(2)=1$，因此我们有 $y=\gamma_m(F(2e),1)=0$,并由 (i) 得出 $x=0$,因而 $y=F(2x)$成立。

我们可假定 $b>0$,由第四章3，（二）有

$$y=F(2e)$$

我们应指出$x=e$。若 $e=0$，则$y=F(0)=0$，再

次从（i)看出 $x=0$。若$e>0$，由第四章1（五）及（i)有

$$e\leqslant 2^{e-1}\leqslant F(2e)=y<t$$

由（vii)我们有

$$x=\gamma_m(u,t)=\gamma_m(g(w,c),t)$$

但由(iii)——(v)容易验证 $t\mid w-2$（$\because$ $t^2\mid r$，有 $t\mid r$，又 $\because$ $r^2-2rs=1+4s^2$，

$$\therefore\ t\mid 1+4s^2$$

由 $w-2=1+(4s+r)s=1+4s^2+rs$

$$\because\ t\mid 1+4s^2+rs,\quad \therefore\ t\mid w-2),$$

因此，由第四章3，（三）有

$$x=\gamma_m(c,t)$$

（从 $t\mid w-2$，$g(w,x)\equiv x\pmod{w-2}$，容易得出

$$g(w,c)\equiv c \bmod t$$

$F(a)\equiv 1\pmod 3$，因而 $t\equiv 1\pmod 3$ 且 $t(24x+1)-1\equiv 0\pmod 3$。这就得出 $F(t(24x+1)-1)$是偶的。令

$$r=F(t(24x+1)),\ s=\frac{1}{2}F(t(24x+1)-1)$$

由第四章3，（一），(iii)被满足。又

$$\because\ (24x+1)F(24x+1)\mid (24x+1)t$$

由第四章2，（五）有

$$(F(24x+1))^2\mid F((24x+1)t)$$

即 $t^2|r$，从而（iv）满足。

接下去，如（v）指出的选择 w，并取

$$u=g(w,x),\quad v=g(w,\ x+1)$$

由第四章3，（三），(vi)保持。

正如本定理证明的前一部分，我们从(iii)——(v) 看出 $t|w-2$。又由第四章3，（二）有：

$$\gamma_m(u,t)=\gamma_m(g(w,x),t)=\gamma_m(x,t)$$

$$\therefore\ \gamma_m(g(w,c),t)=\gamma_m(c,t)$$

又，因为 $t=F(a)$以及 $r=F(2b+1)$，我们从第四章2，（四）有 $t|2b+1$，又由于我们知道$e<t$，我们有

$$x=\gamma_m(c,t)=\gamma_m(q\cdot(2b+1)+e,t)=e$$

这正是我们所需要的。

现在证另一个方向。令 x,y有 $F(2x)=y$，我们寻找 r,s,t,u,v,z,w 满足 (i)—(viii)。

我们选择

$$t=F(24x+1),\quad z=F(24x)$$

很清楚，(i) 是满足的。又，由第四章3，(一)，(ii)也满足。

从斐波那契数的定义，容易看出$F(a)$ 是偶的当且仅当$a\equiv 0\pmod 3$，因此，t 是奇的。还容易看到，如果 $a\equiv 1\pmod 8$，那么但由(i)，我们有$x<t$，因而 $\gamma_m(x,t)=x$，(vii) 式满足。

最后，由(v)有 $4s+r \mid w-3$，又第四章 3，（二）有

$$\gamma_m(u,4s+r)=\gamma_m(g(w,x),4s+r)$$
$$=\gamma_m(F(2x),4s+r)$$

但是，$F(2x)=y$，而由 (i)和 (iv)有 $y<4s+r$，因此，$\gamma_m(u,4s+r)=y$，(viii)满足． □

注意，这里用到的余数函数 $\gamma_m(x,y)$ 是刁藩图的，即谓词 $z=\gamma_m(x,y)$ 是刁藩图的：

$$z=\gamma_m(x,y)\Longleftrightarrow(\exists u)[(x=uy+z) \& (z<y)]$$

我们还指出，容易证明 $y=F(2x)$ 中，一个分量是对另一分量有着指数级的增长，从而 $y=F(2x)$是满足鲁宾逊假设条件的，用简单的归纳法就可完成这一点。

2．幂函数是刁藩图的

我们基于贝尔方程的性质，证明幂函数是刁藩图的，这是鲁宾逊的工作。

考虑下面一个刁藩图方程组：

(i) $x^2-(a^2-1)y^2=1$

(ii) $u^2-(a^2-1)v^2=1$

(iii) $s^2-(b^2-1)t^2=1$

(iv) $v=ry^2$

(v) $b=1+4py=a+qu$

(vi) $s=x+cu$

(vii) $t=k+4(d-1)y$

(viii) $y=k+e-1$

那么，我们会证明，贝尔方程的解可以用这一刁藩图方程组表示，从而证明了它的刁藩图性。

定理7·2

对给定的 $a,x,k,a>1$，方程组 (i)—(viii) 在变量 y,u,v,s,t,b,r,p,q,c,d,e 中有解当且仅当$x=x_k(a)$。

证 首先令方程组 (i)—(viii)有解，由(v)有

$$b>a>1$$

其次，由 (i),(ii),(iii) 及第五章引理 4（记为5·4，以下同），存在着 $i,j,n>0$使

$$x=x_i(a),\quad y=y_i(a)$$

$$u=x_n(a),\quad v=y_n(a)$$

$$s=x_j(b),\quad t=y_j(b)$$

由 (iv)，$y\leqslant v$，所以 $i\leqslant n$。

由 (v)和 (vi)产生同余式：

$$b\equiv a \pmod{x_n(a)}$$

$$x_j(b)\equiv x_i(a) \pmod{x_n(a)}$$

由引理5·15，还得到

$$x_j(b)\equiv x_j(a) \pmod{x_n(a)}$$

代入有：

$$x_i(a)\equiv x_j(a)\pmod{x_n(a)}$$

由引理5·24有：

$$j\equiv \pm i\pmod{4n} \qquad (1)$$

其次，由方程 (iv) $v=ry^2$ 可得：

$$(y_i(a))^2 | y_n(a)$$

又由引理5·12有

$$y_i(a) | n$$

由（1）有：

$$j\equiv \pm i\pmod{4y_i(a)} \qquad (2)$$

由方程(v)，有

$$b\equiv 1\pmod{4y_i(a)}$$

$$\therefore\ 4y_i(a) | b-1$$

由引理5·14，

$$y_j(b)\equiv j\pmod{b-1}$$

$$\therefore\ y_j(b)\equiv j\pmod{4y_i(a)} \qquad (3)$$

由方程 (vii)，

$$y_j(b)\equiv k\pmod{4y_i(a)} \qquad (4)$$

组合（2）、（3）、（4）有

$$k\equiv \pm i\pmod{4y_i(a)} \qquad (5)$$

由方程 (viii)产生

$$k\leqslant y_i(a)$$

并由引理5·18有：

$$i\leqslant y_i(a)$$

又因为数

$$-2y+1,\ -2y+2,\ \cdots,-1,0,1,\cdots,2y$$

构成一个对模 $4y=4y_i(a)$ 的一个互不同余的完全系，由此得出，（5）式必有$k=i$。因而

$$x=x_i(a)=x_k(a).$$

反之，若 $x=x_k(a)$，令 $y=y_k(a)$，因此(i)式成立。令 $m=2ky_k(a)$，并令

$$u=x_m(a),\ v=y_m(a)$$

那么，(ii)式满足。由引理5·9和5·11，

$$y^2|v,$$

这是因为 $v=y_m(a)=y_{2ky_k(a)}(a)$，因而我们可以选择 r满足 (iv)式。又由引理 5·16，v是偶的，而 u必为奇的，且由引理5·7有$(u,v)=1$，由此推出 $(u,4yv)=1$，这是因为，如若不然，令 p 为u与 $4y$的素因子，因 u是奇的，所以$p|y$，由于 $y|v$，有 $p|v$，这与u,v互素矛盾。

由中国剩余定理，我们可以找到 b_0，其中，

$$b_0\equiv1\pmod{4y}$$

$$b_0\equiv a\pmod{u}$$

于是

$$b_0+4juy\equiv1\pmod{4y}$$

$$b_0+4juy\equiv a\pmod{u}$$

令 $b=b_0+4juy$，于是存在着 p,q有：

$$b-1=4yp$$

$$b-a=qu$$

即　　$b=1+4yp=a+qu$

于是存在着 b,p,q而满足 (v)式。

令 $s=x_k(b)$，$t=y_k(b)$，则 (iii) 式满足。

由 $b>a$，$s=x_k(b)>x_k(a)=x$

由 (v)式 $b=a+qu$ 有

$$b\equiv a \pmod{u}$$

由引理5·15有，

$$x_k(b)\equiv x_k(a) \pmod{u}$$

即　　$s\equiv x \pmod{u}$

所以，可选择 c 而满足 (vi)，

$$s=x+cu$$

由引理5·18，$t\geqslant k$，且由引理5·14，

$$t\equiv k \pmod{b-1}$$

由 (v)式，因 $4y$ 是 $b-1$ 的一个因子，所以有

$$t\equiv k \pmod{4y}$$

因而可选择d而满足(vii)式，

$$t=k+4(d-1)y$$

再次使用引理5.18，有 $y\geqslant k$，因而令

$$e=y-k+1$$

可满足 (viii) 式。 □

推论7·3　函数

$$g(z,k)=x_k(z+1)$$

是刁藩图的。

证　在刁藩图方程组 (i)—(viii) 中增加一

个：

$$(*) \qquad a=z+1$$

由上述定理，(∗)，(i)—(viii) 有解当且仅当 $x=x_k(a)=g(z,k)$，于是函数 g 的一个刁藩图定义可使用我们曾叙述过的九个多项式的平方和表示。 □

最后，我们来证明下面的定理。

定理7·4 幂函数$h(n,k)=n^k$ 是刁藩图的。

首先建立下面的不等式：

引理 1

若 $a>y^k$，那么 $2ay-y^2-1>y^k$。

证 若 $y=1$，由$a\geqslant 2$有

$$2ay-y^2-1=2a-2=2(a-1)\geqslant 2>y$$

若 $y\geqslant 2$，$k=1$有：

$$2ay-y^2-1>2y^2-y^2-1=y^2-1>y$$

对于 $k\geqslant 2$，$y\geqslant 2$有：

$$2ay-y^k>2y^{k+1}-y^k=y^k(2y-1)>y^2+1$$

$$\therefore\ 2ay-y^2-1>y^k$$ □

现在在方程 (i)—(viii) 上增添下面四个方程：

(ix) $\quad (x-y(a-n)-m)^2=(f-1)^2(2an-n^2-1)^2$

(x) $\quad m+g=2an-n^2-1$

(xi) $\quad w=n+h=k+l$

(xii) $a^2-(w^2-1)(w-1)^2z^2=1$

引理2

$m=n^k$ 当且仅当方程组(i)—(xii)在其余的变量中有解。

证 假定 (i)—(xii)成立，由xi，$w>1$，因此，$(w-1)z>0$，且由 (xii)，$a>1$。因之可应用定理7·2，得到：

$$x=x_k(a),\ y=y_k(a)$$

由 ix 有，

$$x-y(a-n)-m\equiv 0 \pmod{2an-n^2-1}$$

$$x-y(a-n)\equiv m \pmod{2an-n^2-1}$$

由引理5·17有，

$$x-y(a-n)\equiv n^k \pmod{2an-n^2-1}$$

$$\therefore\ m\equiv n^k \pmod{2an-n^2-1}$$

由 (xi)得出，

$$k,n<w$$

由 (xii)并使用引理5·4，对某个 j有，

$$a=x_j(w),\ (w-1)z=y_j(w),$$

由引理5·14有，

$$y_j(w)\equiv j \pmod{w-1}$$

$$\because\ y_j(w)\equiv 0 \pmod{w-1}$$

$$\therefore\ j\equiv 0 \pmod{w-1}$$

$$\therefore\ j\geqslant w-1$$

由引理5·19，

$$a \geqslant w^{w-1} > n^k$$

由 (x)，$m < 2an - n^2 - 1$

由上面的引理 1，

$$n^k < 2an - n^2 - 1$$

由于 m 和 n^k 同余并都小于模，因而它们必相等，即

$$m = n^k$$

反之，假定 $m = n^k$，解应该由 (i)—(xii) 找到。为此，选择这样的数 w，

$$w > n \text{ 且 } w > k$$

令 $a = x_{w-1}(w)$，于是 $a > 1$

由引理5·14

$$y_{w-1}(w) \equiv w - 1 \pmod{w-1}$$

即 $$y_{w-1}(w) \equiv 0 \pmod{w-1}$$

于是，我们可以写做为：

$$y_{w-1}(w) = z(w-1)$$

因而满足 (xii)。又，令

$$h = w - n, \quad l = w - k$$

则 (xi) 被满足。

同前所述，$a > n^k$，再次应用引理 1，有

$$m = n^k < 2an - n^2 - 1$$

并且 (x) 可满足。令 $x = x_k(a)$，$y = y_k(a)$ 由引理5·17并注意到 $m = n^k$，我们可以确定这样的 f，

$$x - y(a - n) - m = \pm(f - 1)(2an - n^2 - 1)$$

于是(ix)被满足。最后，由定理 7·2，(i)—(viii)可以满足。 □

定理7·4从上述引理 2 立刻得到。 □

3. 三个重要的刁藩图函数

下面我们要证明三个重要的函数是刁藩图的，我们已经看到，在定义刁藩图函数（或谓词）我们可以使用逻辑联接词

$\&, \vee$

但不能使用“—”（¬），可以使用存在量词“∃”但不可使用全称量词“∀”，由于我们已建立了幂函数是刁藩图的，它是可以使用的。还有，我们前面已说明过的函数——是刁藩图函数，都可以使用。

定理7·5 （鲁宾逊）

函数 $f(n,k)=\binom{n}{k}$是刁藩图的。

在证明这个定理的过程中，我们需要建立三个引理。

令 α是实数，$[\alpha]$表示唯一的这样的整数：

$[\alpha]\leqslant\alpha<[\alpha]+1$

引理1 对于 $0<k\leqslant n$，$u>2^n$

则 $\lfloor (u+1)^n/u^k \rfloor = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}$

证

$$(u+1)^n/u^k = \sum_{i=0}^{n} \binom{n}{i} u^{i-k} = S + R$$

这里

$$S = \sum_{i=k}^{n} \binom{n}{i} u^{i-k}, R = \sum_{i=0}^{k-1} \binom{n}{i} u^{i-k}$$

那么，S 显然是个整数，而且

$$R < u^{-1} \sum_{i=0}^{k-1} \binom{n}{i}$$

$$< u^{-1} \sum_{i=0}^{n} \binom{n}{i}$$

$$= u^{-1}(1+1)^n$$

$$< 1$$

所以，

$$S \leqslant (u+1)^n/u^k < S+1$$

$$\therefore \lfloor (u+1)^n/u^k \rfloor = S = \sum_{i=k}^{n} \binom{n}{i} u^{i-k} \qquad \square$$

引理 2

对于 $0<k\leqslant n$，$u>2^n$，则

$$[(u+1)^n/u^k] \equiv \binom{n}{k} \pmod{u}$$

证 由引理1，对所有 $i>k$ 的项，均可为 u 整除，从而 S 被 u 除余 $\binom{n}{k}$。 □

引理3 函数 $f(n,k)=\binom{n}{k}$ 是刁藩图的。

证 因为

$$\binom{n}{k} \leqslant \sum_{i=0}^{n} \binom{n}{i} = 2^n < u$$

由引理2，可决定 $\binom{n}{k}$ 是唯一的 $[(u+1)^n/u^k]$ 模 u 的正剩余，且小于 u，因此

$$z=\binom{n}{k} \Longleftrightarrow (\exists u,v,w,)(v=2^n \,\&\, u>v$$
$$\& \, w=[(u+1)^n/u^k] \,\&\, z\equiv w \pmod{u} \,\&$$
$$z<u)$$

为了看出 $\binom{n}{k}$ 是刁藩图的，只需看右端存在量词内的每个表达式。"&"是刁藩图谓词，$v=2^n$ 由前面的定理自然是刁藩图的，而不等式 $u>v$ 是刁藩图的，因为：

$$u>v \Longleftrightarrow (\exists x)(u=x+v)$$

还有，

$$z\equiv w \pmod{u} \,\&\, z<u \Longleftrightarrow (\exists x,y)$$

$$(w=z+(x-1)u \& u=x+y)$$

最后， $w=[(u+1)^n/u^k]$

$$\Longleftrightarrow$$

$$(\exists x,y,t)(t=u+1 \ \& \ x=t^n \ \& \ y=u^k \&$$
$$w \leqslant x/y < w+1)$$

而且， $w \leqslant x/y < w+1 \Longleftrightarrow wy \leqslant x < (w+1)y$

这就证明了$\binom{n}{k}$是刁藩图的。 □

定理7·6 （鲁宾逊）

函数 $n!$ 是刁藩图的。

引理 4 若 $r>(2x)^{x+1}$，那么

$$x!=[r^x/\binom{r}{x}]$$

证 令 $r>(2x)^{x+1}$，那么

$$r^x/\binom{r}{x}=\frac{r^x x!}{r(r-1)\cdots(r-x+1)}$$

$$=x!\left\{\frac{1}{\left(1-\frac{1}{r}\right)\cdots\left(1-\frac{x-1}{r}\right)}\right\}$$

$$<x!\cdot\frac{1}{\left(1-\frac{x}{r}\right)^x}$$

而，

$$\frac{1}{1-\frac{x}{r}}=1+\frac{x}{r}+\left(\frac{x}{r}\right)^2+\cdots$$

$$=1+\frac{x}{r}\left\{1+\frac{x}{r}+\left(\frac{x}{r}\right)^2+\cdots\right\}$$

$$<1+\frac{x}{r}\left\{1+\frac{1}{2}+\frac{1}{4}+\cdots\right\}$$

$$=1+\frac{2x}{r}$$

又，$\left(1+\frac{2x}{r}\right)^x=\sum_{j=0}^{x}\binom{x}{j}\left(\frac{2x}{r}\right)^j$

$$<1+\frac{2x}{r}\sum_{j=1}^{x}\binom{x}{j}$$

$$<1+\frac{2x}{r}\cdot 2^x$$

所以，

$$r^x/\binom{r}{x}<x!\ +\frac{2x}{r}\cdot x!\,2^x$$

$$<x!\ +\frac{2^{x+1}x^{x+1}}{r}$$

$$<x!+1$$ □

引理 5 $n!$ 是刁藩图的。

证 $m=n!\Longleftrightarrow$

$(\exists r,s,t,u,v)\{s=2x+1\,\&\,t=x+1\,\&\,r=s^t$

$\&\ u=r^n\,\&\,v=\binom{r}{n}\&\,mv\leqslant u<(m+1)v\}$

这里用了引理 4，由于前面已证明 r^n，$\binom{r}{n}$是刁藩图的，所以阶乘函数也是刁藩图的。 □

定理7·7 〔5〕

函数 $h(a,b,y)=\prod_{k=1}^{y}(a+bk)$ 是刁藩图的.

先证明

引理 6 令 $bq\equiv a \pmod M$，那么

$$\prod_{k=1}^{y}(a+bk)\equiv b^y y!\binom{q+y}{y} \pmod M$$

证

$$\because\ b^y y!\binom{q+y}{y}=b^y(q+y)(q+y-1)\cdots(q+1)$$

$$=(bq+yb)(bq+(y-1)b)\cdots(bq+b)$$

$$\equiv(a+yb)(a+(y-1)b)\cdots(a+b) \pmod M$$

□

引理 7 $h(a,b,y)=\prod_{k=1}^{y}(a+bk)$ 是一个刁藩图的函数。

证 在引理 6 中，选择 $M=b(a+by)^y+1$ 那么，$(M,b)=1$ 且 $M>\prod_{k=1}^{y}(a+bk)$。因此，对 q 而言，同余式

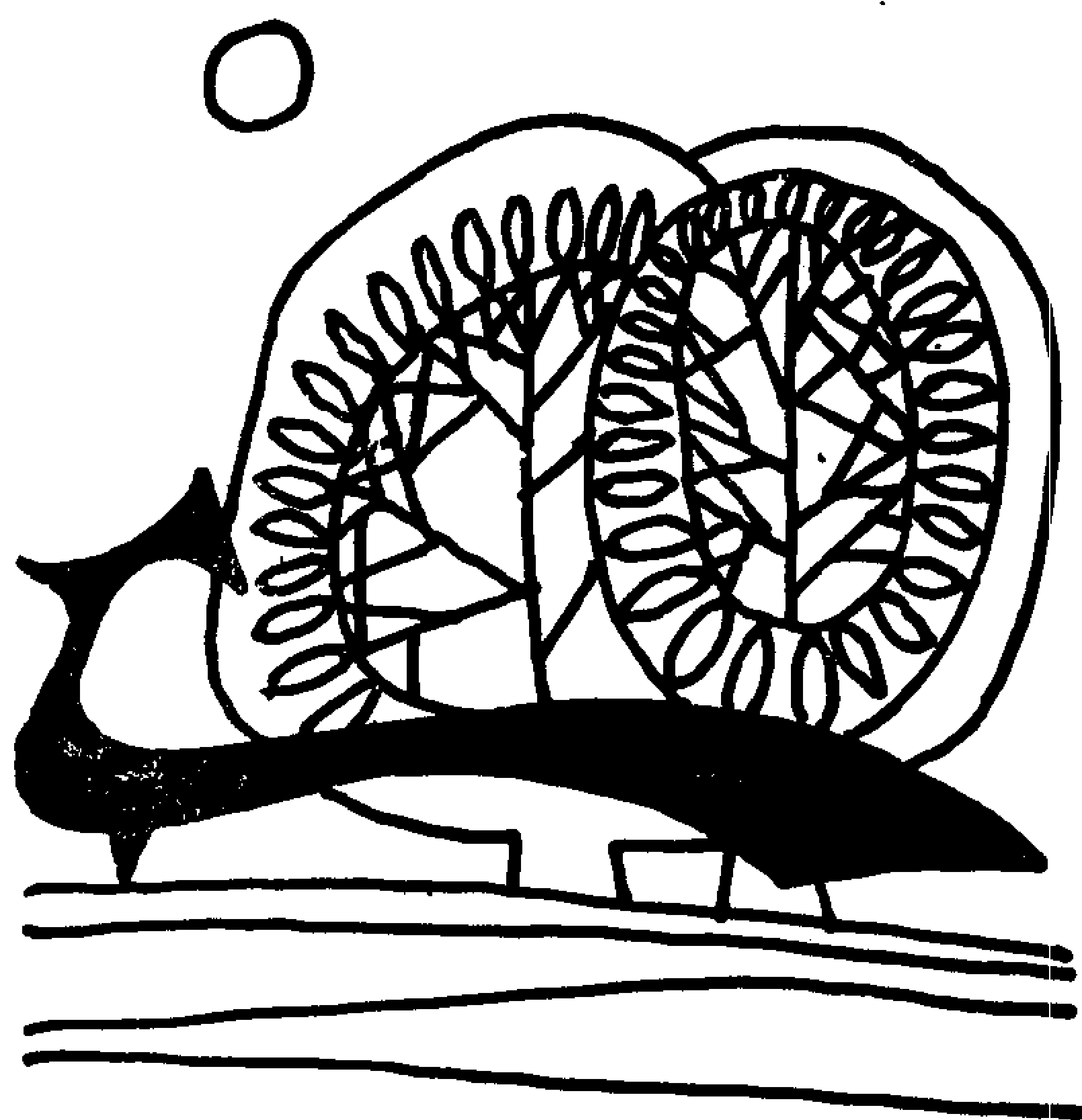
$$bq \equiv a \pmod M$$

可解，并且可确定$\prod_{k=1}^{y}(a+bk)$是唯一的数，它对模M同余于$b^y y!\binom{q+y}{y}$，即：

$$z=\prod_{k=1}^{y}(a+bk) \Longleftrightarrow (\exists M,p,q,r,s,t,u,v,w,x)\{r=a+by \& s=r^y \& M=bs+1 \& bq=a+Mt \& u=b^y \& v=y! \& z<M \& w=q+y \& x=\binom{w}{y} \& z+Mp=uvx\}$$

使用前面已说过的幂函数，$v=y!$，$x=\binom{w}{y}$都是刁藩图的，于是引理即定理得证。

八　受囿量词定理



我们已经知道，刁藩图谓词是可以使用&，
∨，∃的，还有其他的逻辑上使用的运算

$\neg, \forall x, \rightarrow$

于是后面我们会明白，使用这些操作得到的表达式定义的集合是非刁藩图的。

还有两个量词，是在存在量词及全称量词上加上一些限制，即它们不超过某界限，我们称为受囿量词，它们的定义如下：

"$(\exists y)_{<x}\cdots$"意思是"$(\exists y)(y\leqslant x \& \cdots)$"

"$(\forall y)_{<x}\cdots$"意思是"$(\forall y)(y>x\vee\cdots)$"

前者称受囿存在量词，后者称为受囿全称量词。

1．受囿量词定理的原始证明

下面我们会看到，这些运算产生的表达式所定义出的集合，还是刁藩图的。这就是我们下述的受囿量词定理，它也是征服希尔伯特第十问题的最重要的一步。

定理8·1 〔5〕

如果 P 是一个多项式，

$$R=\{\langle y,x_1,\cdots,x_n\rangle \mid (\exists z)_{<y}(\exists y_1,\cdots,y_m)$$
$$[P(y,z,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]\}$$

$$S=\{\langle y,x_1,\cdots,x_n\rangle \mid (\forall z)_{<y}(\exists y_1,\cdots,y_m)$$
$$[P(y,z,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]\}$$

那么，R 和 S 都是刁藩图的。

证 R 是刁藩图的是显而易见的，这是因为：

$$\langle y,x_1,\cdots,x_n\rangle\in R \Longleftrightarrow (\exists z,y_1,\cdots,y_m)$$
$$(z\leqslant y \,\&\, P=0)$$

定理的另一半的证明是相当复杂的。我们先建立两个引理。

引理1

$$(\forall k)_{<y}(\exists y_1,\cdots,y_m)[P(y,k,x_1,\cdots,x_n,y_1,$$
$$\cdots,y_m)=0]$$
$$\Longleftrightarrow$$
$$(\exists u)(\forall k)_{<y}(\exists y_1,\cdots,y_m)_{<u}[P(y,k,x_1,\cdots,$$
$$x_n,y_1,\cdots,y_m)=0]$$

证 等价式的右边推出左边是显而易见的，反之，假定对给定的$y,x_1,\cdots,x_n$，左端是真的，那么，对每个$k=1,2,\cdots,y$存在着确定的数$y_1^{(k)}$，$\cdots,y_m^{(k)}$使

$$P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0$$

取 u为这 my个数

$$\{y_j^{(k)} \mid j=1,2,\cdots,m;\ k=1,2,\cdots,y\}$$

中最大的一个，于是得出，等价式的右端也是真的。 □

引理 2

如果 $Q(y,u,x_1,\cdots,x_n)$ 是有下列性质的多项式：

（1）$Q(y,u,x_1,\cdots,x_n)>u$

（2）$Q(y,u,x_1,\cdots,x_n)>y$

（3）$k\leqslant y$ 且 $y_1,\cdots,y_m\leqslant u$ 则

$$|P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)|\leqslant Q(y,u,x_1,\cdots,x_n)$$

那么

$$(\forall k)_{<y}(\exists y_1,\cdots,y_m)_{<u}[P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]$$

$$\Longleftrightarrow$$

$$(\exists c,t,a_1,\cdots,a_m)[1+ct=\prod_{k=1}^{y}(1+kt)\,\&\,t=Q(y,u,x_1,\cdots,x_n)!\ \&\ 1+ct\mid\prod_{j=1}^{u}(a_1-j)\,\&\cdots\&\,1+ct\mid\prod_{j=1}^{u}(a_m-j)\ \&\ P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)\equiv 0(\mathrm{mod}\ 1+ct)]$$

证 首先证从右至左，$\Longleftarrow$ 方向：

对每个 $k=1,2,\cdots,y$，令p_k 是 $1+kt$ 的素因子，令 $y_i^{(k)}$ 是 a_i 被$p_k(k=1,2,\cdots,y$; $i=1,2,\cdots,m)$ 除的余数，对每个 k,i 将得到：

(i) $1\leqslant y_i^{(k)}\leqslant u$

(ii) $P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0$,

为了证明 (i)，注意到， $p_k|1+kt, 1+kt|1+ct$,

并且$1+ct\left|\prod\limits_{j=1}^{u}(a_i-j)\right.$，即 $p_k\left|\prod\limits_{j=1}^{u}(a_i-j)\right.$，因为 p_k 是素数，所以 $p_k|a_i-j$ 对某个 $j=1,2,\cdots,u$ 成立，因此

$$j\equiv a_i\equiv y_i^{(k)} \pmod{p_k}$$

因为 $t=Q(y,u,x_1,\cdots,x_n)!$，（2）导出每个$1+kt$ 的因子应该大于 $Q(y,u,x_1,\cdots,x_n)$，所以

$$p_k>Q(y,u,x_1,\cdots,x_n)$$

且由（1），$p_k>u$，因此有

$$j\leqslant u<p_k$$

由于 $y_i^{(k)}$ 是 a_i 被 p_k 除的余数，$y_i^{(k)}<p_k$，所以有

$$y_i^{(k)}=j$$

为了证明 (ii)，首先注意到：

$$1+ct\equiv 1+kt\equiv 0 \pmod{p_k}$$

因此， $k+kct\equiv c+kct \pmod{p_k}$

$$\therefore\ k\equiv c \pmod{p_k}$$

又，我们已经得到

$$y_i^{(k)} \equiv a_i \pmod{p_k}$$

因此，

$$P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)}) \equiv P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)$$
$$\equiv 0 \pmod{p_k}$$

又，$|P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})| \leqslant Q(y,u,x_1,\cdots,x_n) < p_k$

$$\therefore\ P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0$$

这就证明了(ii)，并完成了$\Longleftarrow$方向的证明。

为证明另一方向$\Longrightarrow$，令

$P(y,k,x_1,\cdots,x_n,y_1^{(k)},\cdots,y_m^{(k)})=0$

对每个$k=1,2,\cdots,t$均成立，这里每个$y_j^{(k)} \leqslant u$。

我们令 $t=Q(y,u,x_1,\cdots,x_n)!$，且由于

$$\prod_{k=1}^{y}(1+kt) \equiv 1 \pmod{t}$$

我们可以这样的找到 c，

$$1+ct=\prod_{k=1}^{y}(1+kt)$$

又，注意到，对 $1 \leqslant k < l \leqslant y$，有

$$(1+kt,\ 1+lt)=1$$

因为，令 $p \mid 1+kt$，$p \mid 1+lt$，于是 $p \mid l-k$，从而 $p<y$，但因 $Q(y,u,x_1,\ \cdots,\ x_n)>y$，于是 $p<$

$Q(y,u,x_1,\cdots,x_n)$，从而 $p|t$，但这是不可能的。因此 $1+kt(k=1,2,\cdots,y)$ 形成一个允许的模序列，可应用中国剩余定理：

对每个 i，$1\leqslant i\leqslant m$，数 a_i 有，

$$a_i\equiv y_i^{(k)} \pmod{1+kt}, k=1,2,\cdots,y$$

由上面所述，$k\equiv c \pmod{1+kt}$，因此 $P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)\equiv P(y,k,x_1,\cdots,x_n, y_1^{(k)},\cdots,y_m^{(k)})=0 \pmod{1+kt}$

又，因为数$1+kt(k=1,2,\cdots,y)$是两两互素的，且每个都除得尽 $P(y,c,x_1,\cdots,x_n,a_1,\cdots, a_m)$，所以它们的积也除得尽$P(y,c,x_1,\cdots,x_n, a_1,\cdots,a_m)$，即

$$P(y,c,x_1,\cdots,x_n,a_1,\cdots,a_m)\equiv 0 \pmod{1+ct}$$

最后，

$$a_i\equiv y_i^{(k)} \pmod{1+kt}$$

即，　　$1+kt|\, a_i-y_i^{(k)}$

因为　　$1\leqslant y_i^{(k)}\leqslant u$，所以，

$$1+kt \,\Big|\prod_{j=1}^{u}(a_i-j)$$

再次用诸 $1+kt$ 彼此间是互素的，有

$$1+ct \,\Big|\prod_{j=1}^{u}(a_i-j)$$

于是方向$\Longrightarrow$证毕。

定理8·1的证明。

应用引理1和2，我们首先寻找满足引理2中条件（1），（2），（3）中的多项式Q，为此，令

$$P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=\sum_{r=1}^{N}t_r$$

这里，每个 t_r 有形式：

$$t_r=cy^ak^bx_1^{q_1}x_2^{q_2}\cdots x_n^{q_n}y_1^{s_1}y_2^{s_2}\cdots y_m^{s_m}$$

这里 c是正、负整数。

令 $u_r=|c|y^{a+b}x_1^{q_1}x_2^{q_2}\cdots\cdots x_n^{q_n}u^{s_1+s_2+\cdots+s_m}$

并令，$Q(y,u,x_1,\cdots,x_n)=u+y+\sum_{r=1}^{N}u_r$

则 Q 显然满引理2中的条件（1），（2），（3）。因此：

$$(\forall k)_{<y}(\exists y_1,\cdots,y_m)[P(y,k,x_1,\cdots,x_n,y_1,\cdots,y_m)=0]$$

$$\Longleftrightarrow$$

$$(\exists u,c,t,a_1,\cdots,a_m)\Big[1+ct=\prod_{k=1}^{y}(1+kt)$$

$$\&t=Q(y,u,x_1,\cdots,x_n)!\&1+ct\Big|\prod_{j=1}^{s}(a_1$$

$$-j)\ \&\cdots\&\ 1+ct \,\Big|\, \prod_{j=1}^{u}(a_m-j)\ \&\ P(y,c,$$

$$x_1,\cdots,x_n,a_1,\cdots,a_m)\equiv 0\ (\mathrm{mod}\ 1+ct)\ \Big]$$

$$\Longleftrightarrow$$

$$(\exists u,c,t,a_1,\cdots,a_m,\ e,f,g_1,\cdots,g_m,h_1,\cdots,$$

$$h_m,l)\ \Big[e=1+ct\ \&\ e=\prod_{k=1}^{y}(1+kt)\ \&\ f$$

$$=Q(y,u,x_1,\cdots,x_n)\ \&\ t=f!\ \&\ g_1=a_1-u$$

$$-1\ \&\ g_2=a_2-u-1\ \&\cdots\&\ g_m=a_m-u-1$$

$$\&\ h_1=\prod_{k=1}^{u}(g_1+k)\ \&\ h_2=\prod_{k=1}^{u}(g_2+k)\ \&$$

$$\cdots\ \&\ h_m=\prod_{k=1}^{u}(g_m+k)\ \&\ e\,|\,h_1\ \&\ e\,|\,h_2\ \&$$

$$\cdots\&\ e\,|\,h_m\ \&\ l=P(y,c,x_1,\cdots,x_n,a_1,\cdots,$$

$$a_m)\ \&\ e\,|\,l\ \Big]$$

由定理7·7，这是刁藩图的。 □

这个定理告诉我们，刁藩图谓词对受囿量词是封闭的。

2. 受囿量词定理的一个完美形式

上面的定理，从形式上及其证明上都显得冗

长，下面是戴维斯、马吉雅塞维奇和鲁宾逊[9]给出的一个变种，看起来很完美，证明也短多了。

首先我们写出定理6·2（序列数定理）的一个更直观的显示表示，称哥德尔引理。

引理（哥德尔）

对每一个 a 和一个数列 $a_1,\cdots,a_n$ $(a_i<a)$，则存在着唯一的 b，

$$b<\prod_{i=1}^{n}(1+n!\,a_i)$$

且

$$a_i=R_m(b,\ 1+n!\,a_i),\ i=1,\cdots,n.$$

（这里，$R_m(b,c)$ 是 b 除以 c 的最小非负余数）

从序列数定理可知，这一引理的正确性是明显的，检验一下定理的证明过程，就得出这个显示表达式。

定理 令 $P(x,y,k,z_1,\cdots,z_m)$ 是一个多项式，那么

$$(\forall k)_{<x}(\exists z_1,\cdots,z_m)_{<y}[P(x,y,k,z_1,\cdots,z_m)=0]\Longleftrightarrow(\exists b_1,\cdots,\exists b_m)\left[\binom{b_1}{y+1}\equiv\cdots\equiv\binom{b_m}{y+1}\equiv P(x,y,Q!-1,b_1,\cdots,b_m)\right.$$

$$\equiv 0\left(\bmod\binom{Q! - 1}{x+1}\right)\Bigg] \qquad (1)$$

这里 Q是一个这样的多项式，

$$Q = Q(x,y) > |P(x,y,k,z_1,\cdots,z_m)| + 2x + y + 1 \qquad (2)$$

且对所有的 $k\leqslant x$, $z_1\leqslant y,\cdots,z_m\leqslant y$; 还有$b_1,\cdots,b_m$ 均可选择小于 $\binom{Q! - 1}{x+1}$. （3）

证　首先看看（3）中的条件。我们看到，

$$\binom{Q! - 1}{x+1} = (Q! - 1)\left(\frac{Q!}{2} - 1\right)\cdots\left(\frac{Q!}{x+1} - 1\right) \qquad (4)$$

由于 $Q>x+1$,因而上式的右边的每个因子都是整数。注意到 $Q\geqslant 2x+2$,对 $k\leqslant x$, $Q!/(k+1)$ 均可为小于等于 Q 的素因子整除，因而，一个素数若整除（4）式右端的某一因子，则该素数必大于 Q. 若一个素数整除$(Q!/(i+1))-1$ 和 $(Q!/(j+1))-1$,若它必整除 $|i-j|$, 而$|i-j|\leqslant x<Q$,因而 $i=j$, 所以，（4）式中的诸因子是互素的. 又，令p_k是一个素数且它整除 $(Q!/(k+1))-1$,那么，

$$Q! - 1\equiv k \pmod{p_k} \qquad (5)$$

所以，

$$P(x,y,Q! - 1,b_1,\cdots,b_m)\equiv P(x,y,k,R_m$$

$$(b_1,p_k),\cdots,R_m(b_m,p_k))\ (\mathrm{mod}\ p_k),$$
$$k\leqslant x \qquad (6)$$

现在假设（2）的右端成立，那么，对 $b=b_1,\ \cdots,b_m$，$p_k\,|b(b-1)\cdots(b-y)$，因而 $R_m(b,p_k)\leqslant y$。由（3），（6）式右端的绝对值是小于 Q 的，因而小于 p_k。而（6）式的左端由假设有

$$\mathrm{P}(x,y,Q!-1,b_1,\cdots,b_m)\equiv 0\ (\mathrm{mod}\ p_k)$$

因此，

$$P(x,y,k,R_m(b_1,p_k),\cdots,R_m(b_m,\ p_k))=0$$

于是定理的前一半得证。

反之，假设存在着 $z_{1k}\leqslant y,\cdots,\ z_{mk}\leqslant y$ 使

$$P(x,y,k,z_{1k},\cdots,z_{mk})=0,\ k\leqslant x \qquad (7)$$

由中国剩余定理（注意模是互素的），可以找到 $b_i<\binom{Q!-1}{x+1}$（对 $i=1,\cdots,m$）满足同余式组

$$b_i\equiv z_{ik}\left(\mathrm{mod}\left(\frac{Q!}{k+1}-1\right)\right)\ (\text{对} k\leqslant x) \qquad (8)$$

由于 $z_{ik}\leqslant y$，所以

$$\frac{Q!}{k+1}-1|\ b_i(b_i-1)\cdots(b_i-y)\ (\text{对}\ i=1,\cdots,m) \qquad (9)$$

又因为（9）式中的除数是两两互素的，所以它们的积 $\binom{Q!-1}{x+1}$ 也除的尽（9）式的右边。还有，因为（9）式左边的素因子均大于 Q，而 Q

又大于$y+1$，所以，我们得到

$$\binom{Q!-1}{x+1} \Big| \binom{b_i}{y+1},\quad i=1,\cdots,m$$

最后，由（7）和（8）有，

$$P(x,y,Q!-1,b_1,\cdots,b_m) \equiv P(x,y,k,z_{1k},\cdots,z_{mk}) \left(\bmod\left(\frac{Q!}{k+1}-1\right)\right) \qquad (10)$$

由于（10）式的右边是零，且模是互素的，于是我们有：

$$\binom{Q!-1}{x+1} \mid P(x,y,Q!-1,b_1,\cdots,b_m)$$

从而定理的另一半得证。

为了指出受囿量词定理的用处，我们举一个例子，我们将构造一个如下的超幂集的刁藩图定义。

集合 S 是超幂集，它是集合

$$\{1, 2^2, 3^{3^3}, \cdots\}$$

注意到，$m\in S$当且仅当存在着一个序列

$$t_0, t_1, \cdots, t_n$$

使得 $t_0=1, t_{k+1}=n^{t_k}$（对 $k\leqslant n$）且 $t_n=m$。于是由哥德尔引理，

$$m\in S \Longleftrightarrow (\exists n,b,d)(\forall k)_{<n}[R_m(b,1+d) = 1 \;\&\; R_m(b,1+(k+2)d) = n^{R_m(b,1+(k+1)d)} \;\&\; R_m(b,1+(n+1)d)=m] \qquad (11)$$

（由上面所述的哥德尔引理的显示形式，这里取

$$d=(1+n^m)(n+1)!,\ b<\prod_{i=1}^{n+2}(1+id)\ )$$

由于关系 $x^y=z$，$R_m(x,y)=z$ 都是刁藩图的，我们可把（11）翻译成形式：

$$m\in S\Longleftrightarrow(\exists n,a,d)(\forall k)_{<n}(\exists z_1,\cdots,z_\lambda)$$
$$[P(m,n,a,d,k,\ z_1,\cdots,z_\lambda)=0]\qquad(12)$$

由受囿量词定理，（12）的右边是刁藩图的，从而证明了超幂集是刁藩图的。

九　递归函数



我们知道，人类对数的认识有一个漫长的历史，而与数相伴随而来的是数数和计算，人们最早以绳打结计数，以石子堆堆计数，进而发展成以小竹棍数数和计算，甚至发展成能做多种运算的一种工具。（称为算筹）

计算和数学的发展水平有密切的关系，数学给计算提供了理论和方法，计算还和社会的科学技术发展水平相关，社会在发展，人们的计算能力也在发展，计算范围随之也扩大，而且，人们越来越想用机器代替人来计算，从而促使了计算机的发明，当然最早的计算机（器）是相当简单的，如巴斯卡在十七世纪发明的加法机，主要用于做加法，是一种齿轮组合式的，而于近代发明的电子计算机则是1946年的事了，它已是个庞然大物。

随着科学技术的发展，对计算的认识在逐步深化，究竟什么是计算呢？人们常常用下面的话来描述计算：

一个计算过程是在有穷步内，机械地一步步

执行。

我们把这样的计算称为“能行”可计算，或称之为有一能行算法。

能行可计算的概念并未令人十分满意，人们在寻找计算的“模型”，企图更抽象地刻画计算或更具体地给出适于人们习惯的计算模型，早在本世纪三十年代，各种计算模型纷纷出笼，这其中有：

λ演算（邱吉，1936）

图灵机（图灵，1936）

递归函数（哥德尔、赫尔布朗、克林）

波斯特系统（波斯特，1943）

马尔科夫算法论（马尔科夫，1947）

上面的各种计算模型是从完全不同的角度来刻画计算和可计算的，但后来发现，它们都是等价的，即哪一个“工具”计算出的东西都不比另一个多。于是邱吉和图灵分别提出了一个著名的论题，因之称为邱吉论题或邱吉—图灵论题：

任何可计算函数都是递归函数；

任何可计算函数都是图灵机器可计算的。

上述的论断之所以称为论题是因为它不是一个假设或猜想，更不是一个定理，因这句话中含有一未加数学定义的直观概念“可计算函数”，而递归函数和图灵机器可计算均是有严格的数学定义

的。

论题已提出几十年了，人们越来越相信它是正确的，这是因为后来又建立了许多计算模型全是等价的，而且这些年来还未找到一个反例。

下面我们只介绍递归函数的有关知识，而对其他计算模型感兴趣的读者，可以参考书后列出的有关文献。

1. 原始递归函数

在我们定义原始递归函数之前，先看两个例子。

例1　函数 $f(k)$是这样定义的：

$$\begin{cases} f(1)=1, \\ f(k+1)=2f(k)+1 \quad (k=1, 2, \cdots) \end{cases}$$

函数 $f(k)$ 是可计算的，尽管还没有给出其显式表达式，例如计算 $f(6)$，过程如下：

$$\begin{aligned} f(6) &= 2f(5)+1 \\ &= 2(2f(4)+1)+1 \\ &= 4f(4)+3 \\ &= 4(2f(3)+1)+3 \\ &= 8f(3)+7 \\ &= 8(2f(2)+1)+7 \\ &= 16f(2)+15 \end{aligned}$$

$$=16(2f(1)+1)+15$$
$$=32f(1)+31$$
$$=63$$

这一计算本质是，计算 $(k+1)$ 点上的值只依赖于 k 点的值，依此类推，最后直到 $f(1)$，而最后这一点是已知的。

容易写出 $f(k)$的显示表达式：

$$f(k)=2^k-1$$

例 2　令 $F(k)$ $(k=1,2,\cdots)$ 是斐波那契数，那么 $F(k)$如下定义：

$$\begin{cases} F(1)=1 \\ F(2)=1 \\ F(k+2)=F(k+1)+F(k),(k=1,2,\cdots) \end{cases}$$

于是，对任何正整数值 m，可计算出 $F(m)$ 的值。这除了用上面的定义，也可用加法定理，但都是用比 m小的斐波那契数的值。但同时看到，计算 $F(k+1)$ 不光用到 $F(k)$ 的值（还要用 $F(k-1)$），这是与例 1 的区别。例 1，例 2 都是能行可计算的。

例 3　阿克曼函数

由下式定义一个二元函数$A(x,y)$，它称做阿克曼函数：

$$\begin{cases} A(0, y) = y+1 \\ A(x+1, 0) = A(x, 1) \\ A(x+1, y+1) = A(x, A(x+1, y)) \end{cases}$$

这也是一个可计算函数。

这个函数有最大的特点是函数值增长很快，读者可试着计算$A(4, 3)$就会相信这一点，另一点是定义它的递归式较复杂。

现在我们给出递归函数的一个子类——原始递归函数。

初始函数：

$$C(x) = 1^*, \quad S(x) = x+1$$

$$U_i^n(x_1, \cdots, x_n) = x_i, \quad 1 \leqslant i \leqslant n$$

它们分别叫常函数1，后继函数和投影函数。

复合运算：

对给的函数$g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n)$ 及 $f(t_1, \cdots, t_m)$，令函数

$$h(x_1, \cdots, x_n) = f(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$$

则函数 h 称为是一复合函数。

原始递归：

给了 n元函数 f 和$n+2$元函数 g，由它们产

---

* 许多地方，取 $C(x)=0$ 为初始函数，自然它包含本定义，但这一小区别是非本质的。

生一个函数 $h(x_1, \cdots, x_n, z)$，它满足方程：

$$\begin{cases} h(x_1,\cdots,x_n,1) = f(x_1,\cdots,x_n) \\ h(x_1,\cdots,x_n,t+1) = g(t, h(x_1,\cdots,x_n,t),x_1,\cdots,x_n) \end{cases}$$

当 $n=0$时，f 变为一常数，所以 h 可直接从 g 得到。

定义9·1 函数类 ε 称为是原始递归的，如果初始函数属于 ε，且 ε 对复合运算和原始递归是封闭的。

容易验证许多常见的函数都是原始递归的。

（一）$x+y$ 是原始递归的

要说明它是原始递归的，只要说明它是由初始函数经复合及原始递归算子而得到。

令 $f(x, y)=x+y$，定义 $f(x, y)$为：

$$f(x, 1)=x+1 = S(x)$$

$$\begin{aligned} f(x,y+1) &= x+(y+1) \\ &= (x+y)+1 \\ &= f(x, y)+1 \\ &= g(y, f(x, y), x) \end{aligned}$$

更形式地可用递归式写为：

$$\begin{cases} f(x, 1)=S(x) \\ f(x, y+1)=S(U_2^3(y, f(x, y), x)) \end{cases}$$

这里 $g(u, v, w) = S(U_2^3(u, v, w))$。

（二）$x\cdot y$ 是原始递归的

令 $h(x, y)=x\cdot y$，它可定义如下：

$$h(x, 1)=x$$

$$h(x, y+1)=(x\cdot y)+x$$
$$=g(y, h(x, y), x)$$

更形式地处理如下：

$$\begin{cases} h(x, 1)=x=U_1^1(x) \\ h(x,y+1)=f(U_2^3(y,h(x,y),x),U_3^3(y, h(x, y), x)) \end{cases}$$

这里 $g(u, v,w)=U_2^3(u,v, w)+U_3^3(u,v,w)$

上面定义乘法用了投影函数，加法（前已定义），复合及原始递归式，所以，乘法是原始递归的。

下面我们不再一一详尽形式地列出函数原始递归性的定义，而只是显示的或用递归式表示出。而且，我们谈论在N上处处有定义的（称为全函数）数论函数，为此，在原始递归函数的定义中，初始函数 $C(x)=1$，改为 $C(x)=0$，原始递归式扩大一点，

$$h(x_1, \cdots, x_n, 0) =f(x_1, \cdots, x_n)$$
$$h(x_1,\cdots,x_n,t+1)=g(t,h(x_1,\cdots,x_n,t),x_1, \cdots,x_n)$$

（三）$x!$

阶乘函数的递归式为：

$$0!=1$$

$$(x+1)! = x! \cdot S(x)$$

（四）x^y

为定义 x^y 是 x，y 的全函数，我们约定 $0^0=1$，于是幂函数的递归式为：

$$x^0 = 1$$

$$x^{y+1} = x^y \cdot x$$

（五）$P(x)$

$P(x)$ 称为前驱函数，它定义为：

$$P(x) = \begin{cases} x-1, & \text{当 } x \neq 0 \\ 0, & \text{当 } x = 0 \end{cases}$$

所以，它的递归式为：

$$P(0) = 0$$

$$P(x+1) = x$$

（六）$x \dot{-} y$

$x \dot{-} y$ 的定义是

$$x \dot{-} y = \begin{cases} x-y, & \text{当 } x \geqslant y \\ 0, & \text{否则} \end{cases}$$

它的递归式为：

$$x \dot{-} 0 = x$$

$$x \dot{-} (y+1) = (x \dot{-} y) \dot{-} 1 = P(x \dot{-} y)$$

（七）$|x-y|$

$$|x-y| = (x \dot{-} y) + (y \dot{-} x)$$

用复合及（一），（六），$|x-y|$ 是原始递归的。

（八）$\min(x, y)$

取 x，y 中的小者。

$$\min(x, y)=x \dot{-} (x \dot{-} y)$$

由（六）及复合运算。

（九）$\max(x, y)$

取 x，y中的大者。

$$\max(x, y)=x+(y \dot{-} x)$$

由（一），（六）及复合运算。

（十）$s_g(x)$

符号函数

$$s_g(x)=\begin{cases}0, & \text{若 } x=0\\ 1, & \text{若 } x\neq 0\end{cases}$$

$s_g(x)$ 的递归式为，

$$s_g(0)=0$$

$$s_g(x+1)=1$$

（十一）$\overline{s}_g(x)$

$$\overline{s}_g(x)=\begin{cases}1, & \text{若 } x=0\\ 0, & \text{若 } x\neq 0\end{cases}$$

$$\overline{s}_g(x)=1 \dot{-} s_g(x)$$

由（六），s_g 及复合。

（十二）$\gamma_m(x, y)$

余数函数*，前面几章已遇到这个有用的函数，它是 y 被 x 除的余数，为使其全定义，约定 $\gamma_m(0, y)=y$。我们证明它是原始递归的：

$$\because\ \gamma_m(x,y+1)=\begin{cases}\gamma_m(x,y)+1, \text{当 } \gamma_m(x,y)+1\neq x\\ 0, \text{当 } \gamma_m(x,y)+1=x\end{cases}$$

用递归式定义：

$$\gamma_m(x, 0)=0$$

$$\begin{aligned}\gamma_m(x,y+1)&=(\gamma_m(x,y)+1)\mathrm{s_g}(|x-(\gamma_m(x,y)+1)|)\\&=g(x, \gamma_m(x, y))\end{aligned}$$

这里，$g(x, z)=(z+1)\mathrm{s_g}(|x-(z+1)|)$，$g$ 是原始递归的，从而 $\gamma_m(x, y)$ 是原始递归的。

（十三）$q_t(x, y)$

y 被 x 除的商，且为了全定义，约定 $q_t(0, y)=0$，我们证明商函数是原始递归的。

$$\because\ q_t(x, y+1)=\begin{cases}q_t(x,y)+1, \text{若 } \gamma_m(x,y)+1=x\\ q_t(x, y), \text{若 } \gamma_m(x,y)+1\neq x\end{cases}$$

于是可用递归式定义如下：

$$q_t(x, 0)=0$$

---

* 注意，前面的余数函数 $\gamma_m(x,y)$ 是定义为 x 被 y 除的余数，下面的定义相当于变元互换位置，这是为了方便递归函数使用递归式，统一形式，本质上说是无什么区别的。

$$q_t(x, y+1) = q_t(x, y) + \overline{s_g}(|x - (\gamma_m(x, y)+1)|)$$

（十四） $\mathrm{div}(x, y)$

$\mathrm{div}(x, y)$ 表示 x 可整除 y，它是一个仅取两个值的函数：

$$\mathrm{div}(x, y) = \begin{cases} 1, & 若\ x \mid y \\ 0, & 若\ x \nmid y \end{cases}$$

且我们约定：$0 \mid 0$，但 $0 \nmid y$，若 $y \neq 0$。

由于 $\mathrm{div}(x, y) = \overline{s_g}(\gamma_m(x, y))$

∴ $\mathrm{div}(x, y)$是原始递归的。

为了进一步说明几个函数是原始递归的，我们要做一点必要的准备。

谓词 $P(x_1, \cdots, x_n)$的特征函数是 $C_{P(x_1, \cdots, x_n)}$，如果：

$$C_{P(x_1, \cdots, x_n)} = \begin{cases} 1, 若P(x_1, \cdots, x_n)\ 为真 \\ 0, 若\ P(x_1, \cdots, x_n)为假 \end{cases}$$

定义9·2 谓词 $P(x_1, \cdots, x_n)$ 称为是原始递归的，如果它的特征函数 $C_{P(x_1, \cdots, x_n)}$ 是原始递归的。

定理9·1 谓词$P(x_1, \cdots, x_n)$，$Q(x_1, \cdots, x_n)$是原始递归的，则下列谓词(i)，(ii)，(iii)也是原始递归的。

(i) $\neg P(x_1, \cdots, x_n)$

(ii) $P(x_1, \cdots, x_n)\ \&Q(x_1, \cdots, x_n)$

(iii) $Q(x_1, \cdots, x_n)$

证 (i)令 $C_{P(x_1, \cdots, x_n)}$为 $P(x_1, \cdots, x_n)$ 的特征函数，则$\neg P(x_1, \cdots, x_n)$ 的特征函数为 $1 \dot{-} C_{P(x_1, \cdots, x_n)}$。

(ii)令 $C_{Q(x_1, \cdots, x_n)}$ 表示谓词 $Q(x_1, \cdots, x_n)$的特征函数，则 $P(x_1, \cdots, x_n) \& Q(x_1, \cdots, x_n)$的特征函数为

$$C_{P(x_1, \cdots, x_n)} C_{Q(x_1, \cdots, x_n)}$$

(iii) $P(x_1, \cdots, x_n) \vee Q(x_1, \cdots, x_n)$ 的特征函数为 $\max(C_{P(x_1, \cdots, x_n)}, C_{Q(x_1, \cdots, x_n)})$ 由 C_P, C_Q 是原始递归的，并由 $\dot{-}$，·（乘），max 是原始递归的及使用了复合运算。□

假定$f(x_1, \cdots, x_n, z)$是一函数，称$\sum\limits_{z<y} f(x_1, \cdots, x_n, z)$为有界和，称$\prod\limits_{z<y} f(x_1, \cdots, x_n, z)$为有界积。为了使这两个函数是全定义的，令

$$\sum_{z<0} f(x_1, \cdots, x_n, z) = 0; \prod_{z<0} f(x_1, \cdots, x_n, z) = 1$$

于是可用递归式定义这两个函数：

$$\begin{cases} \sum\limits_{z<0} f(x_1, \cdots, x_n, z) = 0, \\ \sum\limits_{z<y+1} f(x_1, \cdots, x_n, z) = \sum\limits_{z<y} f(x_1, \cdots, x_n, z) \\ \qquad + f(x_1, \cdots, x_n, y) \end{cases}$$

$$\begin{cases}\prod_{z<0} f(x_1, \cdots, x_n, z) = 1. \\ \prod_{z<y+1} f(x_1, \cdots, x_n, z) = \left(\prod_{z<y} f(x_1, \cdots, x_n, z)\right) \\ \qquad \cdot f(x_1, \cdots, x_n, y)\end{cases}$$

于是有定理。

定理9·2 若函数 $f(x_1, \cdots, x_n, z)$是一个全定义的原始递归函数，那么，函数

$$\sum_{z<y} f(x_1, \cdots, x_n, z) \text{和} \prod_{z<y} f(x_1, \cdots, x_n, z)$$

是原始递归的。

现在我们描述另一个有用的函数构造技术，我们记

$$\mu z<y \ (\cdots)$$

意思是，"小于 y的那个最小的z,满足…"，为了使其全定义，当那样的 z不存在时，让它取值为 y,例如，给了一个函数 $f(x_1, \cdots, x_n, z)$，我们可定义一个新函数 g:

$$g(x_1, \cdots, x_n, y) = \mu_{z<y} \ (f(x_1, \cdots, x_n, z) = 0)$$

$$= \begin{cases} \text{满足 } f(x_1, \cdots, x_n, z) = 0 \text{且小于 } y \text{ 的最小的 } z & \text{如果这样的} z \text{ 存在} \\ y & \text{如果不存在这样的} z \end{cases}$$

算子$\mu_{z<y}$称为有限最小运算，或称受囿μ运算。

定理9·3 设 $f(x_1, \cdots, x_n, y)$是一个原始递归函数，那么函数

$$\mu_{z<y}\ (f(x_1, \cdots, x_n, z) = 0)$$

也是原始递归的。

证 考虑函数

$$h(x_1, \cdots, x_n, v) = \prod_{u<v} \mathrm{s_g}(f(x_1, \cdots, x_n, u))$$

对于给了 $x_1, \cdots, x_n, y$，假若有

$$z_0 = \mu_{z<y}\ (f(x_1, \cdots, x_n, y) = 0)$$

那么，容易看出

若 $v<z_0$，那么 $h(x_1, \cdots, x_n, v) = 1$

若 $z_0 \leqslant v < y$，那么 $h(x_1, \cdots, x_n, v) = 0$

因此，z_0 是小于 y 而使 $h(x_1, \cdots, x_n, v) = 1$ 的 v 的个数，即

$$z_0 = \sum_{v<y} h(x_1, \cdots, x_n, v)$$

因而，

$$\mu_{z<y}\ (f(x_1, \cdots, x_n, z) = 0) =$$

$$\sum_{v<y}\Big(\prod_{u<v} \mathrm{s_g}\ (f(x_1, \cdots, x_n, u))\Big)$$

由定理9·2。 □

推论9·4 假设$R(x_1, \cdots, x_n, y)$是原始递归谓词，那么：

(i) $f(x_1, \cdots, x_n, y) = \mu_{z<y} R(x_1, \cdots, x_n, z)$ 是原始递归的。

(ii) $P(x_1, \cdots, x_n, y) \equiv (\forall z)_{<y} R(x_1, \cdots, x_n, z)$

$Q(x_1, \cdots, x_n, y) \equiv (\exists z)_{<y} R(x_1, \cdots, x_n, z)$

是两个原始递归谓词。

证 (i) $f(x_1, \cdots, x_n, y) = \mu_{z<y}(\overline{s}_g(C_{R(x_1, \cdots, x_n, z)}) = 0)$

(ii) $\because C_{P(x_1, \cdots, x_n, y)} = \prod_{z<y} C_{R(x_1, \cdots, x_n, z)}$

而，$Q(x_1, \cdots, x_n, y) \equiv \neg(\forall z)_{<y}(\neg R(x_1, \cdots, x_n, z))$，于是，$f(x_1, \cdots, x_n, y)$，$P(x_1, \cdots, x_n, y)$，$Q(x_1, \cdots, x_n, y)$ 都是原始递归的。（用了定理9·3，9·2，$\overline{s}_g$是原始递归的及原始递归谓词对“$\neg$”运算是封闭的。）

现在回过头来继续讨论原始递归函数。

（十五） $D(x)$

$D(x)$是 x的因子个数，并约定 $D(0)=1$。对 $x=6$ 而言，它有因子 1，2，3，6，所以 $D(6)=4$。不难看出，一般地有：

$$D(x) = \sum_{y<x} \mathrm{div}\ (y, x)$$

由定理9·2及（十四），$D(x)$ 是原始递归的。

（十六） $P_r(x)$

$P_r(x)$ 表示仅取 0，1 两个值的函数，它

表示为：

$$P_r(x)=\begin{cases}1, & \text{当 } x \text{ 是一个素数} \\ 0, & \text{当 } x \text{ 不是一个素数}\end{cases}$$

由于一个素数只有1和它本身为其因子，所以因子数为2，即：

$$P_r(x)=\begin{cases}1, & \text{当 } D(x)=2 \\ 0, & \text{否则}\end{cases}$$

$$\therefore\ P_r(x)=\overline{s_g}(|D(x)-2|)$$

由$\overline{s_g}$，绝对值，$D(x)$是原始递归的，所以$P_r(x)$也是原始递归的。

我们看到，几经周折，费了不小气力才证了"x是一个素数"是原始递归的。（注意，$P_r(x)$本身可看成一个谓词），从集合的观点来看，令

$$P=\{x \mid P_r(x)\}$$

则P是素数的集合，而"$x\in P$?"这件事是可以（原始）递归地判定。我们回忆一下，"$x\in P$"是否是刁藩图的我们尚没有证明，即$P_r(x)$是否是一个刁藩图谓词我们尚待证明，这也暗示我们，素数集合有一定的"复杂"程度，同时，我们以后会比较"x是一个素数"用刁藩图表示和用递归函数表示的难易程度上的差别。

（十七）P_x

P_x 表示第 x 个素数，并且约定 $P_0=0$，于是 $P_1=2$，$P_2=3$，……等等。

我们在（十六）中已指出 $P_r(x)$ 也可视为"x是一个素数，"于是 P_x 可递归地定义 如下：

$$P_0 = 0$$

$$P_{x+1} = \mu_z \leqslant (P_x! + 1)\ (z > P_x \& P_r(z))$$

这就是说，第 0 个素数是 0，且第 $x+1$ 个素数是最小的素数 z，它大于第 x 个素数。

我们对 z满足的界要加以说明，这个界 $P_x!+1$ 是足够大的，即在 P_x 与 $P_x!+1$ 之间至少有一个素数，这是基于欧几里得关于素数是无穷的证明，即 $P_{x+1} \leqslant P_x!+1$。

考虑值 $P_x!+1$，它有两种可能性， 要么是一个素数，要么不是，它如果是个素数，显然它一定大于 P_x，故有 $P_{x+1} \leqslant P_x!+1$；如果它不是素数，它必有一个素因子，而显然这素因子不是 P_1，P_2，…，P_x，因为它们除以 $P_x!+1$ 都余 1，所以有 $P_{x+1} \leqslant P_x!+1$。

自然，这个界是太大了，俄国数学家车比雪夫给出了一个漂亮的界：

$$P_{x+1} < 2P_x$$

但证明起来是足够困难的。

还注意，我们用到了谓词 $x<y$是原始递归的，这一点是容易验证的。

（十八）$(x)_y$

$(x)_y$ 表示 x 的素因子分解中，素数 P_y 上

的指数。如 $x=90$，$y=2$

$$x=90=2\times3^2\times5$$

$$P_y=P_2=3, \quad \therefore (90)_2=2$$

为使其为全函数，我们约定

$$(x)_y=0 \text{ 当 } x=0 \text{或 } y=0$$

于是 $$(x)_y=\mu_{z<x}(P_y^{z+1}\nmid x)$$

这里谓词“$P_y^{z+1}\nmid x$”是原始递归的，从而

$(x)_y$是原始递归的。

我们看看开始举的三个例子。对例1，我们稍加修改：

$$\begin{cases} f(0)=0 \\ f(x+1)=2f(x)+1 \end{cases}$$

这显然是个原始递归函数。

对例2的斐波那契数，我们稍加修改为：

$$\begin{cases} F(0)=0 \\ F(1)=1 \\ F(x+2)=F(x+1)+F(x) \end{cases}$$

我们证明 $F(x)$是原始递归的。

令 $g(x)=2^{F(x)}\cdot3^{F(x+1)}$

则 $$\begin{cases} g(0)=2^{F(0)}\cdot3^{F(1)}=3 \\ g(x+1)=2^{F(x+1)}\cdot3^{F(x+2)} \end{cases}$$

又因为：

$$F(x)=(g(x))_1$$

$$F(x+1)=(g(x))_2$$

$$F(x+2)=F(x)+F(x+1)=(g(x))_1+(g(x))_2$$

$$\therefore\ g(x+1)=2^{(g(x))_2}\cdot 3^{(g(x))_1+(g(x))_2}$$
$$=3^{(g(x))_1}\cdot 6^{(g(x))_2}$$
$$=\varphi(g(x))$$

这里 $\varphi(z)=3^{(z)_1}\cdot 6^{(z)_2}$

$\because$ $\varphi(z)$是原始递归的， $\therefore$ $g(x)$ 是原始递归的（用了指数函数，（十八）及递归式）。

而 $F(x)=(g(x))_1$，再次用（十八），得出$F(x)$是原始递归的。还应注意， $g(0)=3$，这里常数 3 是原始递归的，是极容易证明的。

对于例 3，这是一个较复杂的递归函数，但它不是原始递归函数，证明它是一个递归函数可用邱吉论题，计算它显然有一个能行过程，在有穷步内能计算停止，更形式的证明在给出递归函数的定义是可以完成的，从历史上说，它是阿克曼最先找到的一个非原始递归的递归函数，是一个很有名的例子，关于它是递归函数而非原始递归函数的详细论证可参看可计算性理论的书〔20〕。

2. 递归函数

下面定义最小运算（算子）：

给了函数 $f(x_1, \cdots, x_n, y)$，$g(x_1, \cdots, x_n, y)$，假如对每个 $x_1, \cdots, x_n$，至少存在一个 y 而满足方程

$$f(x_1, \cdots, x_n, y)=g(x_1, \cdots, x_n, y)$$

那么，

$$h(x_1, \cdots, x_n)=\mu_y[f(x_1, \cdots, x_n, y) = g(x_1, \cdots, x_n, y)]$$

h 是满足 $f(x_1, \cdots, x_n, y)=g(x_1, \cdots, x_n, y)$ 的 y 中的最小的一个。

我们上面定义出的函数 $h(x_1, \cdots, x_n)$是处处有定义的，即$h(x_1, \cdots, x_n)$ 是一个全函数，如果对 $(x_1, \cdots, x_n)$ 不总是有定义，即定义出的函数 $h(x_1, \cdots, x_n)$是一个部分函数。

定义9·2 函数类R 称为是递归的（或部分递归的），如果它从初始函数出发，使用复合，原始递归式和最小 μ运算得到。

使用最小 μ运算产生出部分函数时对应着部分递归函数类．这里我们将只用 $h(x_1, \cdots, x_n)$ 是处处有定义的情形。

我们提出的一个重要问题是：刁藩图函数和递归函数是什么关系？在回答这个问题前，我们再举一些显示各自能力的例子。

（一）素数集合是刁藩图的

令 P 为素数集合，则：

$$x\in P \Longleftrightarrow x>1\&(\forall y,z)_{<x}[yz<x\vee yz>x\vee y=1\vee z=1]$$

利用受囿量词定理，P是刁藩图的。

素数的另一刁藩图定义是：

$$x\in P \Longleftrightarrow x>1\&((x-1)!,\ x)=1$$
$$\Longleftrightarrow x>1\&\ (\exists y,\ z,\ u,\ v)\ [y=x-1\&z=y!\ \ \&(uz-vx)^2=1]$$

根据前面的定理6·3，应该存在一个表示素数的多项式 Q，P 恰是 Q 的正整数值域。这样的多项式的显示构造是由马吉雅塞维奇第一个给出的。后面我们还要谈这个问题。

（二）函数

$$g(y)=\prod_{k=1}^{y}(1+k^2)$$

是刁藩图的。

这里，我们使用序列数定理把序列 $g(1)$，$g(2)$，…，$g(y)$ 编码成一个数 u，即

$$S(i,\ u)=g(i),\ i=1,\ 2,\ \cdots,\ y$$

因此，

$$z=g(y)\Longleftrightarrow(\exists u)\{S(1,u)=2\&(\forall k)_{<y}[k=1\ \vee(S(k,u)=(1+k^2)S(k-1,u))]\&z=S(y,u)\}\Longleftrightarrow(\exists u)\{S(1,u)=2\&(\forall k)_{<y}\ [k=1\ \vee(\exists a,\ b,\ c)\ (a$$

$=k-1$ & $b=S(a,\ u)$ & $c=S(k,u)$
& $c=(1+k^2)b)]$ & $z=S(y,\ u)\}$

由于 $S(i,\ u)$ 是刁藩图的，又利用受囿量词定理，知函数$g(y)$是刁藩图的。

（三）$S(i,\ u)$是递归函数

我们将证明序列数函数 $S(i,\ u)$ 是递归函数，特别，它是原始递归函数。

由定理6·2的序列数定理可以看出，

$S(i,u)=R_m(L(u),\ 1+iR(u)),(i=1,2,$
$\cdots,\ n)$

我们只需证明 $R_m(L(u),1+iR(u))$是原始递归函数即可，由本章的（十二）知，$R_m(x,\ y)$ 是原始递归的，我们只需证明 $L(u)$，$R(u)$ 是原始递归的。由配对函数的定义知，

$$\begin{cases} z=P(x,y)=\dfrac{(x+y-1)(x+y-2)}{2}+y \\ x=L(z) \\ y=R(z) \end{cases}$$

$$\therefore\ 2z=(x+y-2)(x+y-1)+2y \qquad (1)$$

$$8z+1=(2x+2y-3)^2+8y$$

$$\therefore\ 2x+2y-3\leqslant\sqrt{8z+1}<2x+2y-1$$

于是 $[\sqrt{8z+1}]$或为$2x+2y-3$，或为$2x+2y-2$

$$\therefore\ [([\sqrt{8z+1}]+1)/2]=x+y-1 \qquad (2)$$

又由（1），

$$x+3y-2=2z-\left(\frac{[\sqrt{8z+1}]-1}{2}\right)^2$$

于是有：

$$\begin{cases} x+y\dot{-}2=\dfrac{[\sqrt{8z+1}]\dot{-}1}{2} \\ x+3y\dot{-}2=2z\dot{-}\left(\dfrac{[\sqrt{8z+1}]\dot{-}1}{2}\right)^2 \end{cases}$$

（我们使用数论函数使用的“$\dot{-}$”代替普通的“—”号。）

令 $Q_1(z)=([\sqrt{8z+1}]\dot{-}1)/2$

$Q_2(z)=2z\dot{-}(Q_1(z))^2$

于是上面的联立方程变为：

$$\begin{cases} x+y\dot{-}2=Q_1(z) \\ x+3y\dot{-}2=Q_2(z) \end{cases} \tag{3}$$

解（3）有：

$$y=(Q_2(z)\dot{-}Q_1(z))/2$$

$$x=(Q_1(z)+2)\dot{-}(Q_2(z)\dot{-}Q_1(z))/2$$

从而只要$Q_1(z)$，$Q_2(z)$是原始递归的，则$L(z)$，$R(z)$ 是原始递归的，而 $Q_1(z)$，$Q_2(z)$ 是原始递归的，关键在于这样的函数

$$[\sqrt{x}]$$

是否是原始递归，这是容易证明的，

$$\because \quad [\sqrt{x}]=\mu_{y<x}((y+1)^2>x)$$

谓词 $(y+1)^2>x$ 是原始递归的，再用定理9·3（要稍加变化），所以 $[\sqrt{x}]$是原始递归的，于是证明了 $L(u),R(u)$是原始递归的，从而证明了$S(i, u)$是（原始）递归的。

现在开始证明一个重要定理，以回答我们前面提出的问题。

定理9·5 一个函数是刁藩图的当且仅当它是递归的。

证 我们知道，对每个固定的常数 k，$C_k(x)=k$是递归的，（这由$C_1(x)$是递归的，$C_{k+1}(x)=C_k(x)+C_1(x)$可得。）+，× 也是递归的，而一个有正整数系数的多项式 $P(x_1, \cdots, x_n)$，它可以对变元使用常数，加法、乘法有限次运算而得到，这里用到了复合运算，因而，任一具有正整系数的多项式是递归的。

现证每一个刁藩图函数都是递归的。令$f(x_1, \cdots, x_n)$是刁藩图的，于是有：

$$y=f(x_1, \cdots, x_n) \Longleftrightarrow (\exists t_1, \cdots, t_m)$$
$$[P(x_1, \cdots, x_n, y, t_1, \cdots, t_m)=Q(x_1, \cdots, x_n, y, t_1, \cdots, t_m)]$$

这里 P，Q是具有正整系数的多项式。对 y，t_1，$\cdots$，t_m 使用序列数定理：

$$f(x_1, \cdots, x_n)=S(1, \mu_u[P(x_1, \cdots, x_n, S(1, u), S(2, u), \cdots, S(m+1, u))$$

$= Q(x_1, \cdots, x_n, S(1, u), S(2, u),$

$\cdots, S(m+1, u))]$

因为P，Q，$S(i, u)$是递归的，使用了复合及最小 μ运算，所以 $f(x_1, \cdots, x_n)$是递归的。

证另一方向。由递归函数的定义，初始函数显然是刁藩图的，因而我们只需证明刁藩图函数对复合，原始递归式和最小 μ 运算是封闭的即可。

复合。如果

$$h(x_1, \cdots, x_n) = f(g_1(x_1, \cdots, x_n), \cdots, g_m(x_1, \cdots, x_n))$$

这里 f，g_1，$\cdots$，g_m是刁藩图的，那么 h也是刁藩图的。因为，

$$y = h(x_1, \cdots, x_n) \Longleftrightarrow (\exists t_1, \cdots, t_m) [t_1 = g_1(x_1, \cdots, x_n) \& \cdots \& t_m = g_m(x_1, \cdots, x_n) \& y = f(t_1, \cdots, t_m)]$$

原始递归。如果

$$h(x_1, \cdots, x_n, 1) = f(x_1, \cdots, x_n)$$

$$h(x_1, \cdots, x_n, t+1) = g(t, h(x_1, \cdots, x_n, t), x_1, \cdots, x_n)$$

并且 f，g，是刁藩图的，那么 h也是刁藩图的。应用序列数定理对 $h(x_1, \cdots, x_n, 1)$，$\cdots$，$h(x_1, \cdots, x_n, z)$进行编码有：

$$y = h(x_1, \cdots, x_n, z) \Longleftrightarrow$$

$(\exists u)\{(\exists v)[v=S(1,u)\ \&v=f(x_1,\cdots,x_n)]\ \&(\forall t)_{<z}[(t=z)\vee(\exists v)(v=S(t+1,u)\&\ v=g(t,\ S(t,u),\ x_1,\ \cdots,x_n))]\&y=S(z,\ u)\}$

由定理8·1（受囿量词定理）及$S(i,\ u)$是刁藩图的，所以，h 也是刁藩图的。

最小μ 运算。如果

$h(x_1,\ \cdots,\ x_n)=\mu_y[f(x_1,\ \cdots,\ x_n,\ y)=g(x_1,\ \cdots,\ x_n,\ y)]$，这里 f，g是刁藩图的，那么 h也是刁藩图的。

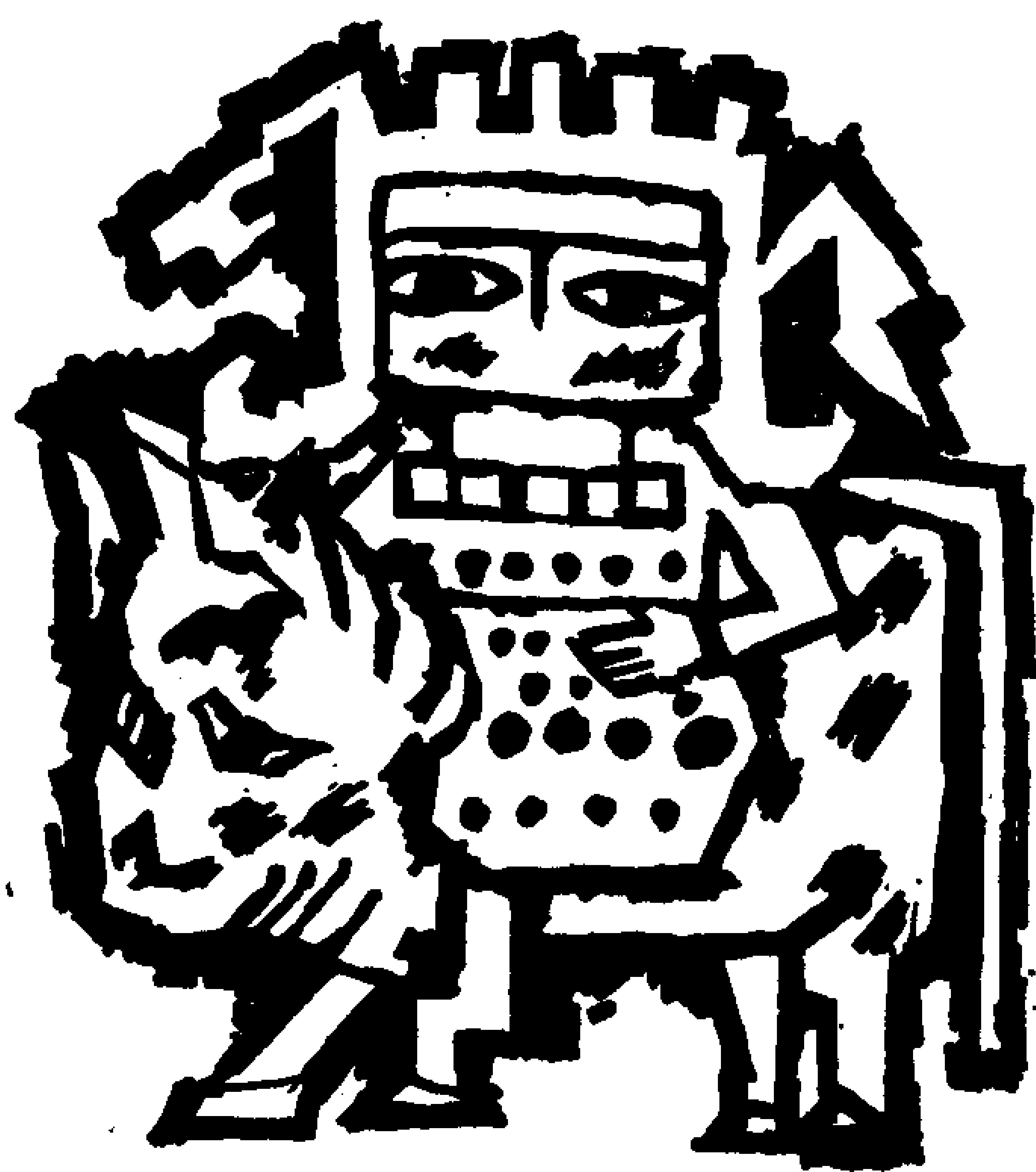
因为，

$y=h(x_1,\ \cdots,\ x_n)\iff$

$(\exists z)[z=f(x_1,\ \cdots,\ x_n,\ y)\ \&z=g(x_1,\ \cdots,\ x_n,\ y)]\ \&(\forall t)_{<y}[t=y\vee(\exists u,v)(u=f(x_1,\ \cdots,\ x_n,\ t)\&\ v=g(x_1,\ \cdots,\ x_n,\ t)\ \&(u<v\vee v<u)]$

再次应用受囿量词定理，$h(x_1,\ \cdots,x_n)$是刁藩图的。 □

十 第十问题是不可解的





本章我们给出希尔伯特第十问题的否定性答案，即希氏第十问题是递归不可解的．这里的“不可解”不是我们不能解，无法解，而是我们严格地从数学上证明对任给一个刁藩图方程它是否有整数解是不存在一个能行有效的过程，即没有一个算法判定一个刁藩图方程有没有整数解。

1. 通用刁藩图集

在说明通用刁藩图集这一概念前，我们先用类似的概念说明更易懂的东西．

有一个一元递归函数（全的）的序列：

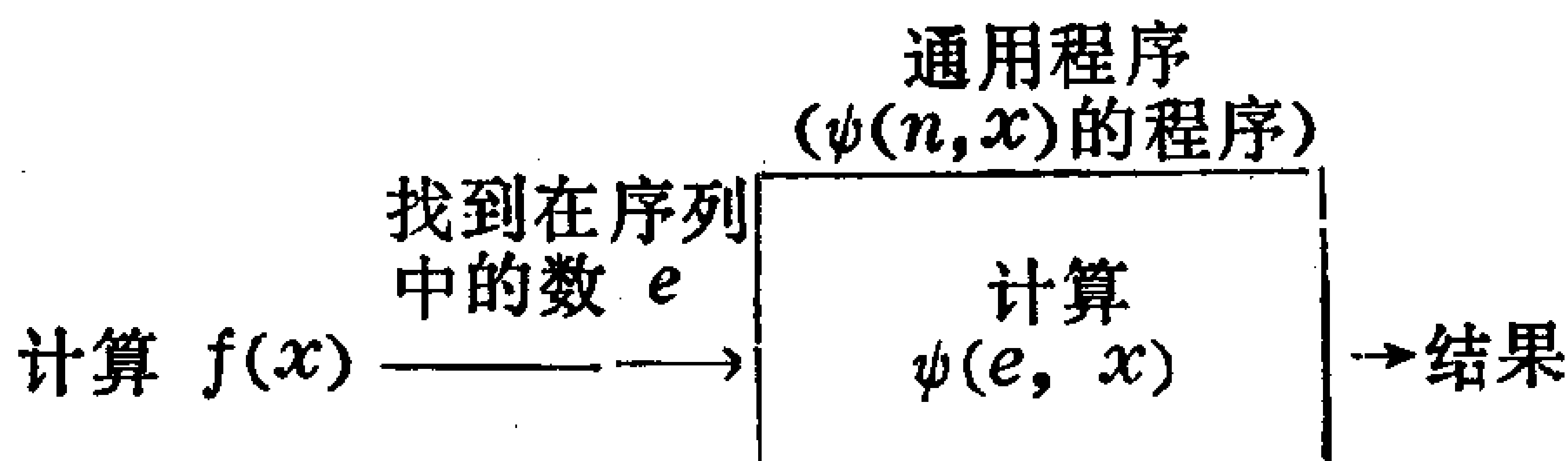
$f_1(x)$，$f_2(x)$，…，$f_k(x)$，…

由邱吉论题，它是可计算的，不妨我们用一个机器（可以是抽象的，也可是具体的）来计算它们，如果我们找到一个二元可计算函数 $\psi(n,x)$，对序列中的任何一个函数 $f_e(x)$，总有

$$\psi(e, x)=f_e(x)$$

我们称$\psi(n, x)$是函数$f_1(x)$，$f_2(x)$，… 的通用

函数。如果我们在某一机器上把 $\psi(n, x)$ 编成程序，则称为通用程序，而计算一函数 $f(x)$ 的过程只需要把某一数 e代入到$\psi(n, x)$ 中的n。示意图如下：



对于正整数子集的所有刁藩图集，我们可以给出一个显式的枚举，为此，我们可以从 1 和变量相继用加法和乘法造出任一有正整数系数的多项式，我们固定变元的字母表：

$$x_0,\ x_1,\ x_2,\ x_3,\ \cdots$$

使用配对函数，可构造上述的所有多项式：

$$P_1 = 1$$

$$P_2 = x_0$$

$$P_{3i} = P_{L(i)} + P_{R(i)}$$

$$P_{3i+1} = P_{L(i)} \cdot P_{R(i)}$$

$$P_{3i+2} = x_i$$

我们记

$$P_i = P_i(x_0,\ x_1\ \cdots,\ x_n)$$

这里 n是足够大的，以使得所有出现在 P_i 中的变量都被包含了，但不一定所有变量都出现。

我们令，

$$D_n=\{x_0|(\exists x_1,\cdots, x_n)[P_{L(n)}(x_0,x_1,\cdots, x_n)=P_{R(n)}(x_0, x_1, \cdots, x_n)]\}$$

这里，$P_{L(n)}$，$P_{R(n)}$ 实际上并不包含所有变量x_0，x_1，…，x_n，但它们不能包含任何其他的变量。（注意 $L(n)$，$R(n)\leqslant n$）。由序列P_i的构造，我们看到，集合的序列

$$D_1, D_2, D_3, D_4, \cdots$$

包含所有的刁藩图集。

定理10·1 （通用定理）

$\{\langle n, x\rangle \mid x\in D_n\}$是刁藩图的。

证 我们使用序列数定理，可以证明：

$$x\in D_n\Longleftrightarrow (\exists u)\{S(1,u)=1\&S(2,u)=x \&(\forall i)_{<n}[S(3i,u)=S(L(i),u)+S(R(i),u)]\&(\forall i)_{<n}[S(3i+1, u)=S(L(i),u)\cdot S(R(i),u)]\&S(L(n),u)=S(R(n),u)\}$$

十分清楚，这等价式的右端是刁藩图的，所以，我们只需证明这等价式是成立的。

对给定的 x，n，若 $x\in D_n$，那么，由D_n的定义，存在着数 t_1，…，t_n 使得：

$$P_{L(n)}(x, t_1, \cdots, t_n)=P_{R(n)}(x,t_1,\cdots,t_n),$$

使用序列数定理，可以选择这样的u，使，

$$S(j, u)=P_j(x, t_1, \cdots, t_n), j=1, 2, \cdots, 3n+2$$

特别是，$S(1, u)=1$，$S(2, u)=x$，

$$S(3i+2, u)=t_i, \quad i=1, 2, \cdots, n$$

因此，等价式的右端是真的。

反过来，如果对给定的 n，x 等价式右端成立，令

$$t_1=S(5,u), t_2=S(8,u), \cdots, t_n=S(3n+2,u)$$

可以推出，

$$S(j, u)=P_j(x, t_1, \cdots, t_n), j=1, 2, \cdots, 3n+2$$

因为 $S(L(n), u)=S(R(n), u)$，

所以，

$$P_{L(n)}(x,t_1,\cdots,t_n)=P_{R(n)}(x,t_1,\cdots,t_n)$$

所以 $x\in D_n$。 □

有了这个通用刁藩图集定理，我们可以构造出一个非刁藩图集。

由于 D_1，D_2，D_3，…枚举出所有的刁藩图集，在集合 $\{1, 2, 3, \cdots, n, \cdots\}$ 中，我们选择出它的一个子集，以构造出一个集合 V。我们问 $1\in D_1$? 若 $1\in D_1$，则不把 1 放在 V 中，若 $1\notin D_1$，则把 1 放在 V 中；接着问 $2\in D_2$?若 $2\in D_2$，则不把它放在 V 中，而 $2\notin D_2$ 时，把 2 放在 V 中，…，对 $n\in D_n$? 若 $n\in D_n$ 则 n 不放在 V 中，否则放在 V 中，等等。

我们这样构造出的集合 V 都至少有一个元素

与每个集合 D_n $(n=1, 2, 3, \cdots)$ 不同，（恰在数 n上），从而构造出一个与 D_1，D_2，D_3，…均不相同的集合，而 D_1，D_2，D_3，… 又是一个所有刁藩图集的一个枚举，从而V不是一个刁藩图集。

形式的论证有，

定义， $V=\{n \mid n \notin D_n\}$，有

定理10·2 V不是刁藩图的。

证 这是康托对角线方法的简单应用。如果V是刁藩图的，那么一定存在着一个 i，使

$V=D_i$，那么 $i \in V$？我们有：

$$i \in V \Longleftrightarrow i \in D_i,\quad i \in V \Longleftrightarrow i \notin D_i$$

这是不可能的。 □

下面我们利用非刁藩图集可以定义出非递归函数，我们定义函数 $g(n, x)$如下：

$$g(n, x)=\begin{cases}1, & \text{若} x \notin D_n \\ 2, & \text{若} x \in D_n\end{cases}$$

则有，

定理10·3 $g(n, x)$ 是非递归的。

证 由定理9·5，如果g是递归的，那么它是刁藩图的。即，

$$y=g(n, x) \Longleftrightarrow (\exists y_1, \cdots, y_m)[P(n, x, y, y_1, \cdots, y_m)=0]$$

$$\therefore\ 1=g(x, x) \Longleftrightarrow (\exists y_1, \cdots, y_m)[P(x,$$

$x, 1, y_1, \cdots, y_m) = 0]$

$\because\ g(x,x) = 1 \Longleftrightarrow x \notin D_x \Longleftrightarrow x \in V$

$\therefore\ V = \{x \mid (\exists y_1, \cdots, y_m)[P(x, x, 1, y_1, \cdots, y_m) = 0]\}$

由定理10·2，V不是刁藩图的，矛盾。 □

应用定理10·1，由于 $x \in D_n$ 是刁藩图的，所以有：

$$x \in D_n \Longleftrightarrow (\exists z_1, \cdots, z_k)\ [P(n, x, z_1, \cdots, z_k)]$$

这里P是依某种方式定义的多项式。

假如有一算法判定刁藩图方程有正整数解，即对希尔伯特第十问题存在着算法，那么，对给定的 n，x，可以使用这个算法判定方程

$$P(n, x, z_1, \cdots, z_k) = 0$$

有没有解。即可判定$x \in D_n$是否成立，因而这一算法可用于计算函数 $g(n, x)$，由邱吉论题，递归函数恰恰是有算法可计算的函数，因而函数 g 是递归的，这与定理10·3相矛盾。这就证明了：

定理10·4 希尔伯特第十问题是不可解的。

希尔伯特第十问题的不可解是指对所有的刁藩图方程找到统一的求解算法，而对特定的一些刁藩图方程类，人们兴趣更浓起来了，特别是数学家贝克由于在这方面的突出贡献，他荣获了1970年的菲尔兹大奖。

我们还注意，由集合V不是刁藩图的这一事实，可有：

$$x\in V \Longleftrightarrow \neg(\exists z_1, \cdots, z_k)[P(x, x, z_1, \cdots, z_k)=0] \Longleftrightarrow \{(\exists z_1, \cdots, z_k)[P(x, x, z_1, \cdots, z_k)=0] \rightarrow 1=0\} \Longleftrightarrow (\forall z_1, \cdots, z_k)[P(x,x,z_1,\cdots,z_k)>0 \vee P(x, x, z_1, \cdots, z_k)<0]$$

这就指出了，使用$\neg$，$\rightarrow$，全称量词之一，均可产生出非刁藩图集。 □

2. 归　约

我们先定义刁藩图集的维数和次数。令S是一个刁藩图集，则存在一个多项式P：

$$S=\{x \mid (\exists y_1,\cdots,y_n)[P(x,y_1,\cdots,y_n)=0]$$

我们把存在的多项式P中的最小的 n称为S的维数，而把诸P中的最小次数的多项式称为S的次数。

定理10·5 每个刁藩图集的次数小于或等于4．（斯柯林[10]）

证 在多项式 $P(x, y_1, \cdots, y_n)$ 中，我们用下列形式的方程：

$$z_j=y_iy_k$$

$$z_j=y_i^2$$

$$z_j = xy_i$$

$$z_j = x^2$$

逐次把P中的变量次数降低,从而可降到2,若把$P=0$ 记为$A=B$,这里 A, B是带有正整系数的多项式，于是可有:

$$A_i = B_i \quad (i=1, 2, \cdots, k)$$

代替 $A=B$,而 A_i, B_i 的次数都不高于2次,从而可组合成一个方程式:

$$\sum_{i=1}^{k} (A_i - B_i)^2 = 0$$

代替那 k 个方程组， 而它的次数显然不会大于4。 □

例 令 $P(x, y_1, y_2)=0$表示为:

$$x^5y^3{}_1 + y^2{}_1y^3{}_2 - 2y^6{}_2 = 0$$

先变成:

$$x^5y^3{}_1 + y_1{}^2y^3{}_2 = 2y^6{}_2 \qquad (*)$$

令, $z_1 = x^2$ (1)

$z_2 = xy_1$ (2)

$z_3 = y_1y_2$ (3)

$z_4 = y_2{}^2$ (4)

(*) 式变成:

$$z_1z_2{}^3 + z_3{}^2y_2 = 2z_4{}^3$$

又令, $z_5 = z_1z_2$ (5)

$$z_6 = z_2^2 \tag{6}$$

$$z_7 = z_3^2 \tag{7}$$

$$z_8 = z_4^2 \tag{8}$$

（*）式进一步变为：

$$z_5 z_6 + z_7 z_2 = 2 z_8 z_4 \tag{9}$$

（1）——（9）都成为

$$A_i = B_i \quad (i = 1, 2, \cdots, 9)$$

的形式，而 A_i，B_i 或为1次或为2次。于是

$$P(x, y_1, y_2) = 0 \text{可用}$$

$$\sum_{i=1}^{9} (A_i - B_i)^2 = 0 \tag{10}$$

来代替，(10)的次数降低为小于等于4，但多引入了8个变量。

下面是关于维数的基本定理。

定理10·6 存在着一个整数m，使每个刁藩图集有维数小于或等于m。

证 由通用定理，

$D_n = \{x \mid (\exists y_1, \cdots, y_m) [P(x, n, y_1, \cdots, y_m) = 0]\}$，于是，对所有的 n，D_n的维数是小于或等于 m的。 □

例 刁藩图集 S_q 定义如下：

$S_q = \{x \mid (\exists y_1, \cdots, y_q) [x = (y_1 + 1) \cdots (y_q + 1)]\}$，这里，$S_2$ 就是合数集合，而 S_q 是"q重"复合数的集合。十分惊奇的是，给出 S_q 的刁藩

图定义可少于 q个参数（对于大q）。[11]

通用刁藩图集的参数有多大呢？直接的计算大约的数为50，但可以大大缩小，马吉雅塞维奇和鲁宾逊证明了下面的定理。[12]

定理10·7 存在着一个通用方程，

$$P(x,\ n,\ y_1,\ \cdots,\ y_{13})=0$$

即任一刁藩图集的维数可以等于13。

维数看来还可以缩小，据说已缩小到9*。

上面我们用次数和维数来考察一个刁藩图方程的复杂情况，还有用验证一个刁藩图方程是否有解需要多少次加法和乘法，即，是用“步数”来度量一个刁藩图方程的复杂度，这方面也有一些进展。

3. 递归可枚举集

什么是刁藩图集？或刁藩图集的类有多大，是考虑的时候了，为此我们给出定义。

定义10·1 一个正整数的n数组的集合S称为是递归可枚举的，如果存在着递归函数 $f(x,\ x_1,\ \cdots,\ x_n)$，$g(x,\ x_1,\ \cdots,\ x_n)$使得：

---

* 吴允增教授说，这可能是一位日本学者的工作，但具体文献未能查到。

$$S=\{\langle x_1, \cdots, x_n\rangle \mid (\exists x)[f(x, x_1, \cdots, x_n) = g(x, x_1, \cdots, x_n)]\}$$

这个定义看起来和它的名字"递归可枚举"是相差很远的，要知道，最初的定义是，对于集合$\{0, 1, 2, \cdots\}$上一个子集S称为是递归可枚举的，如果存在一个递归函数$f(x)$，使它枚举S的每一元素，即

$$S=\{f(0), f(1), f(2), \cdots\}$$

从而S是一个递归函数的值域。

10·1的定义是适于证明下面重要的定理。

定理10·8 集合S是刁藩图的当且仅当它是递归可枚举。

证 如果S是刁藩图的，则存在着两个有正整系数的多项式P，Q，使：

$$\langle x_1, \cdots, x_n\rangle \in S \Longleftrightarrow (\exists y_1, \cdots, y_m)[P(x_1, \cdots, x_n, y_1, \cdots, y_m) = Q(x_1, \cdots, x_n, y_1, \cdots, y_m)] \Longleftrightarrow (\exists u)[P(x_1, \cdots, x_n, S(1, u), \cdots, S(m, u)) = Q(x_1, \cdots, x_n, S(1, u), \cdots, S(m, u))]$$

所以，S是递归可枚举的。

反过来，如果S是递归可枚举的，那么，存在着递归函数$f(x, x_1, \cdots, x_n)$，$g(x, x_1, \cdots, x_n)$使，

$$\langle x_1, \cdots, x_n\rangle \in S \Longleftrightarrow (\exists x)[f(x, x_1, \cdots,$$

$x_n) = g(x, x_1, \cdots, x_n)] \Longleftrightarrow (\exists x, z)$
$[z = f(x, x_1, \cdots, x_n) \& z = g(x, x_1,$
$\cdots, x_n)]$

由定理9·5，S是刁蕃图的. □

由定理10·2，我们立刻有：

定理10·9 存在着非递归可枚举集。

由通用定理，可有递归可枚举集的枚举定理：

有一个多项式（称通用多项式），即

$$P(z, x, y_1, \cdots, y_m)$$

对任一递归可枚举集S，存在一个 n，使

$$x \in S \Longleftrightarrow (\exists y_1, \cdots, y_m)[P(n, x, y_1, \cdots, y_m) = 0]$$

n又称S的指标。

还应提出的是，戴维斯曾给出递归可枚举集的一个表示法，即，任一递归可枚举集S，均可表示为：

$$S = \{x \mid (\exists y)(\forall k)_{<y}(\exists y_1, \cdots, y_m)[P(k, x, y, y_1, \cdots, y_m)]\}$$

这就是著名的戴维斯范式。

后来，阿·鲁宾逊指出，范式中的m可取为4，而马吉雅塞维奇更进一步指出，范式中甚至可取$m = 2$，已知不能取 $m = 0$。可否总有$m = 1$，是尚待解决的问题。

还应指出的是，我们整个的论证，除了用了递归函数的定义和邱吉论题，很少涉及数理逻辑或递归论的深入知识，如果允许我们利用递归函数论的一点结果，是很容易构造出非递归的函数和不可判定的谓词（即递归可枚举而非递归的谓词）。

著名美国数学家克林在本世纪四十年代就建立了下面的所谓范式定理：

存在着一固定的原始递归函数 $U(x)$ 及一原始递归谓词 $T(z, x_1, \cdots, x_k, y)$，任给一 k元递归函数（全函数）$f(x_1, \cdots, x_k)$，总存在着一个数m（与 f 有关），使

(i) $(\forall x_1, \cdots, x_k)(\exists y)\ T(m, x_1, \cdots, x_k, y)$

(ii) $f(x_1, \cdots, x_k) = U(\mu y T(m, x_1, \cdots, x_k, y))$

这个定理说明了，对 k元递归函数，存在着一个 $k+1$ 元的通用函数，这个函数可以枚举所有 k元递归函数。特别 $k=1$，函数

$$U(\mu y T(z, x, y))$$

是所有一元递归函数的通用函数，我们可以容易的指出：

$$U(\mu y T(x, x, y))$$

是一个非递归的函数。

证 如果它是一个递归函数，则

$$g(x) = U(\mu y T(x, x, y)) + 1$$

也是一个递归函数．由于 $U(\mu yT(z,\ x,\ y))$是通用函数，所以存在着某一数m，使

$$g(x)=U(\mu yT(m,\ x,\ y))$$

$$\therefore U(\mu yT(x,x,y))+1=U(\mu yT(m,x,y))$$

令 $x=m$，导出矛盾。 □

这也说明了谓词 $(\exists y)T(x,\ x,\ y)$ 是不可判定的，特别，集合

$$S=\{x\mid(\exists y)T(x,\ x,\ y)\}$$

是一个递归可枚举集，而 $x\in S$ 是不存在一个算法可判定的。由递归可枚举集就是刁藩图集（定理10·8），并注意它的证明只依赖于定理 9·5，所以，对上述的集合S，有一个刁藩图方程$P(x,\ y_1,\ \cdots,\ y_m)=0$，使

$$(\exists y)T(x,\ x,\ y)\Longleftrightarrow(\exists y_1,\ \cdots,\ y_m)[P(x,\ y_1,\ \cdots,\ y_m)=0]$$

由于等价式的左边是不可判定的，从而右边也是不可判定的，即找到了一个特殊的刁藩图方程$P(x,\ y_1,\ \cdots,\ y_m)=0$，对任给一个$x$，它有没有正整数解是没有一个算法可判定的。从而希氏第十问题是不可解的。

十一　素数表示与著名数学问题



下面我们叙述几个有关的问题，它们与刁藩图方程有着密切的联系，并且是十分重要而有趣的。

1. 素数的刁藩图表示

人们对素数的研究是很古老的，古希腊时代，欧几里得发现了关于素数的第一个定理，这就是：素数是无穷的；又有一个叫埃拉托斯散的人，发现了一个求素数的方法，称之为筛法，许多年后，人们对素数并没有什么深入的认识。

人们知道，素数的分布是没有规律的，给出素数总是以“表”的形式，例如，“1000以内的素数表”如下，等等．于是，许多数学家想给出素数的显示表达式，自然更希望找到一个多项式，这多项式的值枚举素数或算出的值都是素数。第一个有名的尝试是法国数学家费马给出的，他声称，型如

$$2^{2^n}+1 \quad (n=0, 1, 2, 3, \cdots)$$

的数都是素数。这对$n=0$，1，2，3，4相应的五个数是3，5，17，257，65537确实都是素数，而当继续验证时，就不再是素数了，1732年，年轻的数学家欧拉指出，费马的断言是错误的，因为，当$n=5$时，

$$2^{2^5}+1=4294967297=641\times 6700417$$

它是个合数。

十分有趣的是，人们再也没有发现这样的费马素数，相反，发现了许多合数，如今，对

$$F(n)=2^{2^n}+1$$

人们反而猜测，当$n\geqslant 5$时，$F(n)$总是合数。由于$F(n)$的增长速度太快，对给定的n，判定$F(n)$是素数还是合数都是一件不容易的事，由于电子计算机的出现，前几年出现一件惊人的事件，计算机“发现”了F(73)是个合数！

人们寻求“素数多项式”更具有“手工”的技巧，人们发现，

$$x^2+x+41$$

对$x=0,1,2,\cdots,39$，给出了40个素数，更有人发现。

$$x^2-79x+1601$$

对$x=0,1,2,\cdots,79$，给出了80个素数。

总之，寻求这种产生有限个素数的代数公式是没有太大的价值的。

素数集合是相当复杂的，我们证明它是个刁藩图集也花费了不少力气，顺便说一句，十九世纪，狄利克雷指出，算术级数中有无穷多个素数，但证明十分困难，而在斐波那契序列中有多少个素数（有穷还是无穷），至今还是个迷。

1960年，普特南首先想到，可找到一个多项式，它的正整数值域恰恰就是素数集，这正是定理6.3所证明的。

从第九章，我们已看到，P是素数集合，则有：

$$x \in P \Longleftrightarrow x > 1 \ \& \ (\exists y, z, u, v)$$
$$[y = x - 1 \ \& \ z = y! \ \& (uz - vx)^2 = 1]$$

又，我们已证明 $z = y!$ 是刁藩图的，不难将等价式的右端变成一个形如：

$$(\exists y_1, \cdots, y_m)[Q(x, y_1, \cdots, y_m) = 0]$$

的刁藩图谓词，再次应用定理6·3，可找到所需的多项式 $Q^*(x, y_1, \cdots, y_m)$。

我们还可以较直观的定义素数，十分清楚，p是素数当且仅当

$$p = s + 1 = r + 2 \qquad (1)$$

$$q = s! \qquad (2)$$

$$ap - bq = 1 \qquad (3)$$

对 a，b，s，r，q 在N中有解。

对 $t \geqslant s$，

$$s! = \frac{t(t-1)\cdots(t-s+1)}{\binom{t}{s}}$$

正如我们在第七章用的方法，只要当 $t \geqslant 2s^{s+2}$，容易验证：

$$s! = \left[\frac{t^s}{\binom{t}{s}} \right]$$

于是可用以列各式代替（2）：

$$t = 2s^{s+2} \quad (4)$$

$$t^s = qu + w \quad (5)$$

$$u = \binom{t}{s} \quad (6)$$

$$u = w + x + 1 \quad (7)$$

因为（5）和（7）对变量 x，w有解当且仅当 $q = [t^s/u]$。

通过方程

$$(y+1)^t = \sum_{i=0}^{t} \binom{t}{i} y^i$$

来定义二项式系数，当 $y > 2^t$ 时，（6）式可被下列各式替换：

$$y = 2^t + 1 \quad (9)$$

$$z = y + 1 \quad (10)$$

$$z^t = ly^{s+1} + uy^s + m \quad (11)$$

$$u + v = 2^t \quad (12)$$

$$m+n+1 \quad = y^s \qquad (13)$$

因此，方程组（1），（3）—（5），（7），（9）—（13）是素数集的幂刁藩图定义。再由第七章，幂函数是刁藩图的，最终可给出素数的刁藩图表示。

决定素数集的多项式出现有不同的形式，第一个是马吉雅塞维奇找到的24个未知数、37次的多项式，后又修改为有21个未知数、21次的多项式。还有一个是具有12个未知数的多项式，自然未知数是要多一些。

更有趣的是，考虑多项式的长度最小，用以测量多项式的复杂度，琼斯给出了一个 325 个符号的多项式〔14〕，我们写下来让读者欣赏，同时也指出这一多项式取素数的关键所在。琼斯构造的多项式如下：

$$(k+2)\{1-([wz+h+j-q]^2+[(gk+2g+k+1)\ (h+j)+h-z]^2+[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2+[2n+p+q+z-e]^2+[e^3(e+2)(a+1)^2+1-0^2]^2+[(a^2-1)y^2+1-x^2]^2+[16r^2y^4(a^2-1)+1-u^2]^2+[((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2]^2+[(a^2-1)l^2+1-m^2]^2+[ai+k+1-l-i]^2+[n+l+v-y]^2+[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m]^2+[g+y(a-p-1)+s(2ap$$

$$+2a-p^2-2p-2)-x]^2+[z+pl(a-p)$$

$$+t(2ap-p^2-1)-pm]^2)\}$$

琼斯的这一多项式是25次，有26个变元，它只取素数的本质上有如下结构：

$$(k+2)\{1-(M_1^2+\cdots+M_\lambda^2)\}$$

由于花括号中不能取负值和零，

$$\therefore\ k+2\text{是素数}\Longleftrightarrow M_1=0\ \&\cdots\&M_\lambda=0$$

我们还看出，这一形式正是普特南定理暗示出的样子。

2. 三大著名问题

数论中有三大著名问题，这就是费马猜想（又称费马大定理）、哥德巴赫猜想和黎曼猜想。它们都是几百年来数学家为之呕心沥血奋斗不息的数学难题，在希氏第十问题解决之后，戴维斯，马吉雅塞维奇和鲁宾逊想到，这些问题可否转化为刁藩图方程，进而从研究解刁藩图方程入手呢。

在长满荒草的原野上，踏出一条或许是成功的小路，他（她）们在暗暗自喜，他们十分乐观，在探索的路上迈出了新的一步。

这是1976年戴维斯等人的想法，十年过去了，当吴允曾教授于1985，1986年两次会晤戴维斯教授时，顺便问起他的这些设想，他说，十

年来并没有什么大的进展，当时想的太乐观了，……。

（一）费马猜想

费马是十七世纪的法国数学家，他本是一名律师而业余酷爱数学，一生发表著作很少，但见解颇多。

1621年，费马买到一本刁藩图所著《算术》的拉丁文译本，在研究了刁藩图方程之后，在此书的边页上写下了几行批注，说：

不可能把一个整数的立方表为两个整数的立方和，也不可能把一个整数的四次幂表为两个整数的四次幂的和，一般说来，不可能把任意一个次数大于2的整数的方幂，表为两个整数的同次方幂之和。

用现在的代数语言说，当$n>2$时，方程

$$x^n+y^n=z^n \tag{14}$$

没有正整数解。

费马自称已发现了这一论断的奇妙的证明，但是他死后，人们并未找到他的任何东西。

三百多年过去了，费马猜想至今还是一个谜。

在方程（14）中，对具体的n，如$n=3,4,5$等等，都是一个特定的刁藩图方程，但对任意的$n>2$，变元出现在指数上，从而（14）实质上

是一个指数方程。我们设法把它变成一个刁藩图方程。

前面我们已经给出幂函数的显式的刁藩图定义，即，我们有一个多项式 $A(a, b, c, w_1, \cdots, w_k)$，

$$A(a, b, c, w_1, \cdots, w_k)=0$$

对未知数 $w_1, \cdots, w_k$ 有解，当且仅当参数 a，b，c，满足条件

$$a=b^c$$

因此，方程（14）对某值n 可解，有方程

$$A^2(p, x, n, w_1, \cdots, w_k)+A^2(q, y, n, v_1, \cdots, v_k)+A^2(p+q, z, n, u_1, \cdots, u_k)=0 \tag{15}$$

有解。因而费马的猜想等价于下面的刁藩图方程，

$$A^2(p, x+1, n+3, w_1, \cdots, w_k)+A^2(q, y+1, n+3, v_1, \cdots, v_k)+A^2(p+q, z, n+3, u_1, \cdots, u_k)=0$$

对 n，p，q，$u_1, \cdots, u_k$，$v_1, \cdots, v_k$，$w_1, \cdots, w_k$，x，y，z在非负整数中无解。因此，只要对这个方程有一个判定算法，则对费马猜想就可解决。

容易写出方程（15）的显式式，事实上，柔恩[13]给出了这个方程，它有72个变元，并占用

了几乎一页纸。其后，按照马吉雅塞维奇和鲁宾逊的思想，该方程的变元可缩小至12。

（二）哥德巴赫猜想

二百多年前，德国一位中学数学教师哥德巴赫发现了一个奇妙的现象，于1742年6月7日，他写信给住在俄国彼得堡的大数学家欧拉，问到大于等于6的偶数均可表示为两个奇素数的和吗？欧拉在回信中，肯定了这一猜想无疑是正确的，但他并未给出证明。于是命题“每个大于2的偶数是两个素数之和”，这就是哥德巴赫猜想。

每一个充分大的偶数可以表示为一个素数与一个素因子个数不超过 C 的数之和，我们记为 $(1+C)$，于是哥德巴赫猜想简记为“1 + 1”。

这个问题是出奇的困难，长期以来，它一直被人们誉为“皇冠上的明珠”，在探索证明这一猜想的道路上，留下了不少中外数学家的足迹，其中苏联数学家布赫斯塔勃，维诺格拉朵夫做出了许多贡献，我国数学家陈景润、王元、潘承洞也做出了突出的贡献，他们的出色成绩荣获了国家科学奖金。

陈景润的结果最初发表在1966年，被誉为陈氏定理：

任何一个大偶数，总可表为一个素数与另一个不超过两个素数之积的和。

人们通俗地称为“1 + 2”。

二十多年过去了，陈氏定理仍处于领先地位，但也未能登上这最后的一步！*

哥德巴赫猜想之所以如此困难，是由于命题是用加法的方式叙述的，而素数又是由乘法来刻画的，在自然数中，一般说来，乘法性质和加法性质之间难于建立起联系。说的更清楚些，比如下面给出的一个加法和乘法的联系，足见一斑：

用加法，递归式定义乘法，令$\varphi(x,y)=x+y$，$f(x, y)=xy$，则：

$$\begin{cases} f(x, 0)=0 \\ f(x, y+1)=\varphi(x, f(x, y)) \end{cases}$$

我们已经知道，递归式的能力是很强的。

又，可用·（乘法）和S（后继）来定义加法。

$$z=x+y \Longleftrightarrow S(Sx\cdot Sz)\cdot S(y\cdot Sz)=S(Sz\cdot Sz\cdot S(Sx\cdot y))$$

用简单的多项式乘法是容易验证等价式的正确性。

现在回到哥德巴赫猜想，我们先构造一个习

---

* 1986年9月，王元教授在南开大学校园内的一次私人谈话中说：“1 + 1”和“1 + 2”不是一回事，意指不能用“1 + 2”的方法解决“1 + 1”的问题。

潘图方程，

$$B(p, w_1, \cdots, w_k)=0 \quad (16)$$

它对变元 $w_1, \cdots, w_k$ 是可解的当且仅当 p 是素数，容易验证，方程

$$(u+1)(1-B^2(p_1, w_1, \cdots, w_k)-B^2(p_2, w'_1, \cdots, w'_k)-(2u+4-p_1-p_2)^2-t)=a \quad (17)$$

对所有的非正数 a是可解的(此时，可有$u=0, t=-a$, $p_1=p_2=2$, $w_1, \cdots, w_k$, $w'_1, \cdots, w'_k$ 由（16）中当 $p=2$ 时的一个解决定），并对那些且仅对那些正数a，而 $2a+2$是两个素数的和可解($u=a-1$, $t=0$, $p_1+p_2=2a+2$, $w_1, \cdots, w_k$ 和 $w'_1, \cdots, w'_k$ 分别由方程（16）对相应的$p=p_1$ 和 $p=p_2$ 的解而决定）。于是哥德巴赫猜想可表示为，方程（17）左端的多项式，当变元取值为非负整数时，表示每一个整数。对诸变元应用拉格郎日定理，于是有，当变元取整数值时这多项式取每一个整数时，当且仅当哥德巴赫猜想成立。

我们还注意到，许多著名的数学问题都有形式，

$$\forall n P(n)$$

这里 $P(n)$是某一递归（可判定）谓词，哥德巴赫猜想也不例外，令 $P_r(x)$表示“x是素数”

（前面我们曾用过这一符号），于是哥德巴赫猜想可表示为：

$$(\forall n)(\exists x)(\exists y)\ [P_r(x)\&P_r(y)\&(2n+2=x+y)]$$

这里应注意，在寻找x，y使 $x+y=2n+2$ 的过程中，x，y是有界的，即 $x\leqslant 2n$，$y\leqslant 2n$，于是上面的公式可重新写为：

$$(\forall n)(\exists x)_{<2n}(\exists y)_{<2n}[P_r(x)\&P_r(y)\&(2n+2=x+y)]$$

从而，

$P(n)=(\exists x)_{<2n}(\exists y)_{<2n}[P_r(x)\&P_r(y)\&(2n+2=x+y)]$，于是 $P(n)$ 是原始递归的，是可判定的。

（三）黎曼猜想

黎曼是十九世纪的德国数学家，是现代几何的创始人，他提出了一个著名的猜想：

复变数s 的函数

$$\zeta(s)=\sum_{n=1}^{\infty}n^{-s}$$

的所有非平凡零点均位于 $\mathrm{Re}(s)=\frac{1}{2}$的直线上（这里 $\mathrm{Re}(s)$ 表示 s 的实数部分），后者又可等价地表示为：

$\zeta(s)$在带形区域 $1/2<\mathrm{Re}(s)<1$中永不等

于零。

黎曼猜想似乎表示为（$\forall n$）$R(n)$（$R(n)$ 是递归的）有困难，然而可以把它表示为下述等价的命题：

对所有的 n，（$n=1, 2, 3, \cdots$）

$$\left(\sum_{k<\delta(n)} \frac{1}{k} - \frac{n^2}{2}\right)^2 < 36n^3 \qquad (18)$$

其中，
$$\delta(x) = \prod_{s<x}\prod_{j<s}\eta(j)$$

而

$$\eta(j) = \begin{cases} 1, & \text{当 } j \text{ 不是一个素数幂} \\ p, & \text{当 } j = p^k\text{，其中} p \text{为素数} \end{cases}$$

于是我们可以把该命题简记为

$$(\forall n)R(n)$$

其中 $R(n)$ 显然是可判定的。

由于 $(\forall n)R(n) \Longleftrightarrow \neg(\exists n)\overline{R(n)}$，而 $\overline{R(n)}$ 也是可判定的，于是可得到一个显式的刁藩图方程，它没有解恰恰使（18）总成立。

自然，我们并不能把每一个著名问题都归约为一个刁藩图方程的不可解性，例如，对于孪生素数*是无穷的猜想可表示为：

---

* 孪生素数是指 p 和 $p+2$ 均为素数，如 3，5；5，7；11，13；等等。

$$(\forall n)\{(\exists p)[p>n \,\&\, P_r(p) \,\&\, P_r(p+2)]\}$$

显然花括号中的谓词并非是递归的，可是我们给出一个加强的命题：

$$(\forall n)\{(\exists p)[n+4<p<2^{n+4} \,\&\, P_r(p) \,\&\, P_r(p+2)]\}$$

这时，花括号中的谓词是可判定的，从而加强的孪生素数猜想可变换为一个特定的刁藩图方程的不可解性。

3. 两个未解决的问题

我们已经知道，每个刁藩图方程均可归约到一个次数≤4的方程，又人们对于次数为2而未知数数目为任意的刁藩图方程存在着算法，于是自然产生的未解决问题：

1° 对于三次方程而言，希尔伯特第十问题可判定吗？

另一个未解决的问题是：

2° 是否存在可以用来判定任一刁藩图方程是否有有理数解的算法？

自然还有一些未解决的问题，我们不便一一列举了。

参 考 文 献

〔1〕 Julia Robinson,

Existential definability in arithmetic,

Trans.Amer.Math.Soc.,72(1952),437—449.

〔2〕 Martin Davis,

Arithmetical problems and recursively enumerable predicates, J. Symbolic Logic, 18 (1953) 33—41.

〔3〕 ——,

Computability and Unsolvability McGraw Hill, New York, 1958

(中译本：可计算性与不可解性，

沈泓等译，吴允曾校，北京大学出版社，1984)

〔4〕 Martin Davis, Hilary Putnam,

Reduction of Hilbert's tenth problem, J. Symbolic Logic, 23 (1958) 183—187.

〔5〕 Martin Davis, Hilary Putnam, and Julia Robinson,

The decision problem for exponential Diophantine equations, Ann. Math.,74 (1961) 425—436.

〔6〕 Ю. В. Матиясевич,

Доклады Академии Наук СССР 1970. том 191. № 2, 279—282.

〔7〕——,

ДАН, 1971. ТОМ 196, № 4, 770—773.

〔8〕Martin Davis,

Hilbert's tenth problem is unsolvable, Amer. Math. Monthly, 80 (1973), 233—269.

〔9〕Martin Davis, Yuri Matijasevič and Julia, Robinson,

Hilbert's tenth Problem. Diophantine Equations:Positive Aspects of A Negative Solution, Proceedings of Symposia in Pure Mathematic Volume 28, 1976, 323—377.

〔10〕Th. Skolem,

Diophantische Gleichungen, Ergebnisse d. Math. U. Ihrer Grenzgebiete, Bd. 5, Julius Springer, 1938.

〔11〕Georg Kreisel,

Mathematical Reviews, 24 (1962) Part A, P. 573 (review number A 3061).

〔12〕Yuri Matijasevič and Julia Robinson,

Reduction of an arbitrary Diophantine equation to one in 13 unknowns, Acta Arithmetica 27 (1974), 521—553.

〔13〕Keijo Ruohnen,

Hilbert's tenth problem (Finnish), Arkhimedes (Helsinkfors) 1972, 71—100.

〔14〕James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens,

Diophantine reprentation of the Set of prime numbers, Amer. Math. Monthly, to appear.

〔15〕胡世华，陆钟万
数理逻辑基础，科学出版社，1983。
〔16〕S.C. 克林著，莫绍揆译
元数学导论，科学出版社，1985。
〔17〕华罗庚
数论导引，科学出版社，1979。
〔18〕王浩
数理逻辑通俗讲话，科学出版社，1981。
〔19〕Nigel Cutland,
COMPUTABILITY
An introduction to recursive function theory, Cambridge University Press 1980.
〔20〕张鸣华
可计算性理论，清华大学出版社，1984。
〔21〕高恒珊
关于 D. Hilbert 第十问题的递归不可解性（内部），1972.
〔22〕杨东屏
递归论介绍，数理化信息（1），135—141，辽宁教育出版社，1985.
〔23〕莫绍揆
从Hilbert第十问题谈起——介绍数理逻辑的两个有名结果，数理化信息（2），辽宁教育出版社，1986。
〔24〕H.德里
100个著名初等数学问题
——历史和解，上海科技出版社，1982。
〔25〕吴振奎
斐波那契数列，辽宁教育出版社，1987。
〔26〕胡久稔
数学趣题与BASIC程序，辽宁教育出版社，1985。

中外人名译名索引

刁藩图	Diophantus
马尔科夫	Марков, А. А.
马吉雅塞维奇	Матиясевич, Ю. В.
贝尔	Pell, John
贝克	Baker, Alan
巴斯卡	Pascal, Blaise
车比雪夫	Чебышев, П. Л.
布赫斯塔勃	Бухштаб, А. А.
毕达格拉斯	Pythagoras
邱吉	Church, Alonzo
克林	Kleene, Stephen C.
阿克曼	Ackermann, Wilhelm
阿基米德	Archimedes
希尔伯特	Hilbert, David
欧拉	Euler, Leonhard
舍弗	Sheffer, H. M.
图灵	Turing, Alan Mathison
波斯特	POST, Emil L.
法尔廷斯	Falting
欧儿里得	Euclid
拉格郎日	Lagrange, Joseph Louis
埃拉托斯散	Eratosthenes
莱辛	Lessing, G. E.

康托	Cantor, Georg
哥德尔	Gödel, Kurt
哥德巴赫	Goldbach, Christian
菲尔兹	Fields, John Charles
维诺格拉朵夫	Виноградов, А. И.
琼斯	Jones, James P.
斯柯林	Skolem, Thoralf
普特南	Putnam, Hilary
费马	Fermat, Pierre de
斐波那契	Fibonacci, Leonardo
鲁宾逊（杰）	Robinson, Julia
鲁宾逊（阿）	Robinson, Raphael M.
赫尔布朗	Herbrand Jacques
黎曼	Riemann, George Friedrich
戴维斯	Davis, Martin
柔恩	Ruohnen, Keijo